2010-09

Arctic region policy information sharing : model options

Marie, Claire.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ARCTIC REGION POLICY: INFORMATION SHARING MODEL OPTIONS

by

Claire Marie

September 2010

Thesis Advisor:	Robert Simeral
Second Reader:	Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2010	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Arctic Region Policy: Information Sharing Model Options	
6. AUTHOR(S) Claire Marie	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number ___N.A._____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

Continued climate change and minimum ice conditions over the past several years is allowing for increased maritime activity in the Arctic, which may lead to potential homeland security/defense missions. In January 2009, the U.S. government acknowledged the probability of these missions with an updated *Arctic Region Policy*, which highlighted the need to develop capabilities to protect U.S. air, land and sea borders, military/civilian vessels and aircraft, maritime commerce, critical infrastructure and key resources. Successfully supporting these missions will depend on a coherent understanding of all the activities taking place in the Arctic region. Achieving this level of "situational awareness" will only be possible when all equity partners and stakeholders are sharing relevant information. This thesis examined three popular information-sharing models, Alaska Information Analysis Center, Joint Interagency Coordination Group, and the Alaska Partnership for Infrastructure Protection to determine which would work best for a broad array of Arctic partners and stakeholders. The thesis' research and analysis shows that none of the models are sufficient or stand-alone; rather a megacommunity is necessary, consisting of all equity partners interfacing with the stakeholders, managed by leaders that will motivate the community to achieve a high degree of awareness for all Arctic activity.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Arctic region policy, interagency, collaboration, information sharing, megacommunity, Joint Interagency Coordination Group, Alaska Information Sharing and Analysis Center, Alaska Partnership for Infrastructure Protection, fusion center, information sharing strategies	151
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ARCTIC REGION POLICY: INFORMATION SHARING MODEL OPTIONS

Claire Marie
Chief, Joint Operations Center, Alaskan Command/Joint Task Force, Alaska
B.S., University of Maryland, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Claire Marie

Approved by: Robert Simeral
Thesis Advisor

Lauren Wollman
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Continued climate change and minimum ice conditions over the past several years is allowing for increased maritime activity in the Arctic, which may lead to potential homeland security/defense missions. In January 2009, the U.S. government acknowledged the probability of these missions with an updated *Arctic Region Policy*, which highlighted the need to develop capabilities to protect U.S. air, land and sea borders, military/civilian vessels and aircraft, maritime commerce, critical infrastructure and key resources. Successfully supporting these missions will depend on a coherent understanding of all the activities taking place in the Arctic region. Achieving this level of "situational awareness" will only be possible when all equity partners and stakeholders are sharing relevant information. This thesis examined three popular information-sharing models, Alaska Information Analysis Center, Joint Interagency Coordination Group, and the Alaska Partnership for Infrastructure Protection to determine which would work best for a broad array of Arctic partners and stakeholders. The thesis' research and analysis shows that none of the models are sufficient or stand-alone; rather a megacommunity is necessary, consisting of all equity partners interfacing with the stakeholders, managed by leaders that will motivate the community to achieve a high degree of awareness for all Arctic activity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AICC	Alaska Information Coordination Center
AKIAC	Alaska Information and Analysis Center
AKSHSS	Alaska State Homeland Security Strategy
ALCOM	Alaskan Command
AMSA	Arctic Marine Shipping Association
APIP	Alaska Partnership for Infrastructure Protection
ARCUS	Arctic Research Consortium of the United States
ASD	Assistant Secretary of Defense
AST	Alaska State Troopers
ATACA	Anti-Terrorism Advisory Council of Alaska
CIA	Central Intelligence Agency
CoI	Community of interest
CONOPS	Concept of operations
CRS	Congressional Research Service
DHS	Department of Homeland Security
DHS&EM	Division of Homeland Security and Emergency Management
DHS ISS	Department of Homeland Security Information Sharing Strategy
DHS OIG	Department of Homeland Security Office of the Inspector General
DIME	Diplomatic, informational, military, economic
DIMES	Diplomatic, informational, military, economic, state
DMVA	Department of Military and Veterans Affairs
DoD	Department of Defense
DoD ISS	Department of Defense Information Sharing Strategy
DOJ	Department of Justice
DoS	Department of State
DPS	Alaska Department of Public Safety

EO	Executive Order
EOC	Emergency operation center
FBI	Federal Bureau of Investigation
FBI INISS	Federal Bureau of Investigation National Information Sharing Strategy
FEMA	Federal Emergency Management Agency
FC	Fusion center
GAO	Government Accounting Office
HD	Homeland defense
HLS	Homeland security
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IARPC	Interagency Arctic Research Policy Committee
IAPG	Interagency Arctic Policy Group
IC	Interagency coordination
IC	U.S. Intelligence Community
IC ISS	Intelligence Community Information Sharing Strategy
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISC	Information Sharing Council
ISE	Information Sharing Environment
ITACG	Interagency Threat Assessment Coordination Group
JFCOM	U.S. Joint Forces Command
JIACG	Joint Interagency Coordination Group
JTF-AK	Joint Task Force Alaska
LEISP	Department of Justice Law Enforcement Information Sharing Program
MOU	Memorandum of understanding
NCTC	National Counterterrorism Center
NOAA	National Oceanic and Atmospheric Administration

NORAD	North American Aerospace Defense Command
NSPD	National Security Presidential Directive
NSIS	National Strategy for Information Sharing
NSMS	National Strategy for Maritime Security
OIG	Office of Inspector General
ODNI	Office of the Director of National Intelligence
PBS	Public Broadcasting Service
PDD	Presidential Decision Directive
PM	Program manager
PM-ISE	Program Manager—Information Sharing Environment
RADM	Rear Admiral
SIPRNet	Secret Internet protocol router network
SITREPs	Situation reports
SoA	State of Alaska
SOP	Standard operating procedure
UNCLOS	United Nations Convention on the Law of the Sea
USARC	U.S. Arctic Research Commission
USCG	U.S. Coast Guard
USCG D17	U.S. Coast Guard District 17
USEIA	U.S. Energy Information Administration
USFFC	U.S. Fleet Forces Command
USGS	U.S. Geological Survey
USG	U.S. government
USN	U.S. Navy
USNORTHCOM	U.S. Northern Command
USNC IC	U.S. Northern Command Interagency Coordination

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my co-workers: thank you for putting up with my absence from work, and especially Julian Jensen, for listening to me pontificate about the Arctic. I also want to thank the leadership, especially COL John Buss, who went the extra mile to ensure an incredible opportunity to expand my knowledge.

To my mentors: CAPT Simeral and Drs. Bellavita and Wollman, who had great patience for me throughout this program.

To my cohorts in 0901/0902, especially Lisa and Jody, thank you for putting up with my “Arctic-centric” mindset, and for providing comfort for an out of place, rural Alaskan in the middle of urban America.

I would also like to thank my amazing parents, Joe and Wanda, who have ceaselessly encouraged me to pursue lifelong education, in addition to providing an infinite amount of grounded wisdom throughout my life.

Finally, to my brilliant and loving children, Michelle, David and Sara, siblings, and best friends Karen and Jim: thank you for tolerating my sequestered lifestyle and also putting up with my ranting about nonstop homework for the past 18 months. I could not have completed this program without all your support and love.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

On January 29, 2009, *Homeland Security Presidential Directive 25/National Security Presidential Directive 66* (HSPD 25/NSPD 66) *Arctic Region Policy* was issued. Geographically, this policy covers approximately one sixth of the earth's landmass; more than 30 million km^2 and includes two major shipping lanes (Arctic Council, 2009). The area spans 24 time zones with a population of about four million, including over 30 different indigenous peoples and dozens of languages (Arctic Council, 2009). In addition to the United States, Russia, Norway, Canada, Iceland and Denmark also have defense, homeland security and resource interests in this region; some of these are conflicting territorial claims as shown in Figure 1.

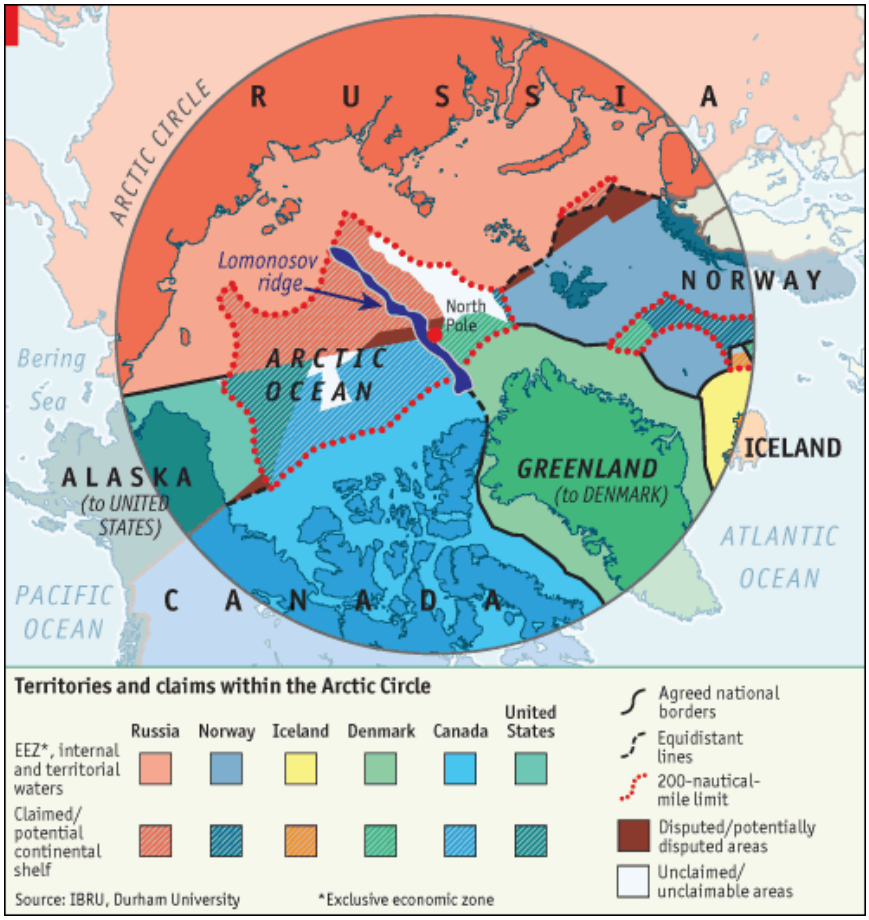

Figure 1. Territories and Claims Within the Arctic Circle (From The Scramble for the Seabed, 2009)

According to the chairman of the U.S. Arctic Research Commission, there are four forces of change leading to an "accessible Arctic." These include climate, technologies (e.g., transport, satellite communication, navigation, remote sensing), global demand for Arctic resources, and Arctic residents reaching to improve life (Treadwell, 2009, p. 37). One example of the accessible Arctic can be seen in the amount of activity, as shown in Figure 2.

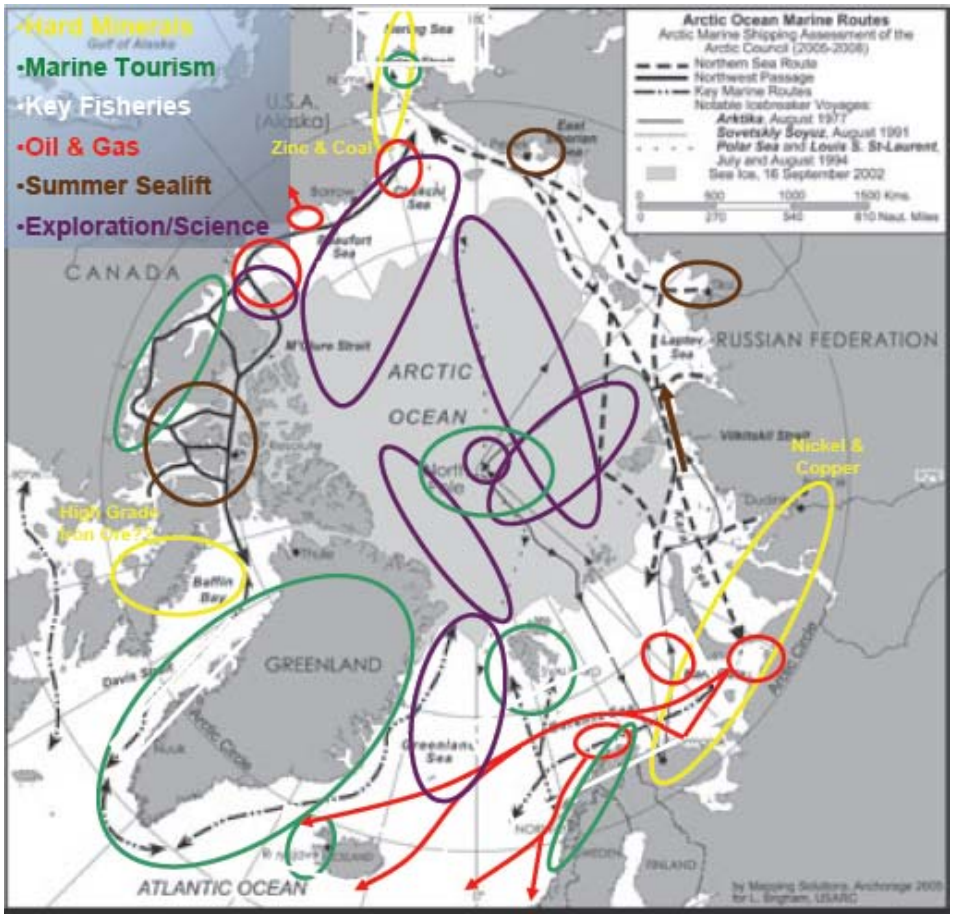

Figure 2. Arctic Activity (From Ellis, 2009, p. 8)

HSPD 26/NSPD 66, the fourth policy iteration, brings awareness to the potential impact that these accessibility "forces" have for all, including those with malevolent intentions. Accordingly, the government added the Department of Homeland Security (DHS) to support homeland security (HLS) missions, in addition to the homeland defense (HD) missions that the Department of Defense (DoD) had been responsible for since the first policy. The new policy highlights the need to develop capabilities to protect U.S. air, land and sea borders, military/civilian vessels and aircraft, maritime commerce, critical infrastructure and key resources in the Arctic region. The complexity in supporting this policy can be viewed through a cursory lens of economic, political/military, scientific activities and interest in the area.

1. Economics

The total mean undiscovered conventional oil and gas resources of the Arctic are estimated to be approximately 90 billion barrels of oil, 1,669 trillion cubic feet of natural gas and 44 billion barrels of natural gas liquids (U.S. Geological Survey, 2008). For comparison, worldwide consumption of petroleum products was 82.3 million barrels a day in 2004, with the top three consumers being the United States (20.7 million), China (6.4 million) and Japan (5.4 million) (U.S. Energy Information Administration [USIA], 2010).

In 2007, the U.S. maintained a similar consumption rate (average of 20.7 million barrels of oil a day), approximately 40 percent of that (9.29 million) was for motor vehicles (USIA, 2010). Americans used more oil for their motor vehicles than the total combined amounts of Russia, Canada, the United Kingdom and France (Public Broadcasting Service [PBS], 2010) The U.S. represents about five percent of the human population but consumes a quarter of the world's oil (PBS, 2010). U.S. petroleum consumption dropped slightly in 2008, to 19.4 million barrels, still a considerable amount considering that the country only produced 4.95 million barrels of crude oil per day (USIA, 2008). Motor gasoline consumption that year continued to be high at 8.9 million barrels/378 million gallons a day (USIA, 2008). The important point to note is the steady U.S. appetite for oil, which could be a driving factor for Arctic exploration.

In order to obtain the rights to these undersea Arctic resources, the 1982 U.N. Convention on the Law of the Sea (UNCLOS) treaty must be ratified. After that, each signatory nation has 10 years to map the seabed. Those maps, along with sediment samples and other scientific information, can be used to claim parts of the seabed that are extensions of the continental shelf of each nation. Rear Admiral (RADM) Brooks, former Commander of US Coast Guard District 17 (USCG D17) in Juneau, Alaska, summed up the importance of signing the treaty:

> The Convention guarantees our military and transportation industries critical navigation and overflight rights, U.S. fishermen exclusive fishing out to 200 nautical miles, and much, much more. In the view of the Coast Guard, the Convention for the Law of the Sea greatly improves our ability to protect the American public as well as our efforts to manage our ocean resources and to protect the marine environment. (Brooks, 2009)

Even though the U.S. has not ratified UNCLOS, it continues to map the Arctic area along with other nations attempting to define their territory and the resources contained therein. The economic as well as national security importance of the region is depicted in Figure 3.

Figure 3. Potential Future Arctic Shipping Routes (From Treadwell, 2009, p. 18)

2. Political/Military

In addition to the UNCLOS treaty ratification, several political incidents over the past few years have heated up the region. For example, according to the *London Times*, in 2007 the Canadian Prime Minister, Stephen Harper, "ordered military ships to the Arctic amid growing tensions with both the United States and Russia over competing territorial claims in the region" (Blomfield,

2008). The same article claims that “Russia has raised the stakes in the international scramble for the Arctic by announcing it will boost its military presence in the region to protect its ‘national interests’” (Blomfield, 2008). The willingness of Russia to incur the high risk of planting a flag on the North Pole seabed in 2007 was another sign of political interest that raised the attention of several Arctic neighbors (Struck, 2007).

The investments made by Russia in their fleet of 25 polar icebreakers (six active heavy icebreakers, two heavy icebreakers in caretaker status, 15 other icebreakers, and two additional icebreakers leased from the Netherlands) points toward their commitment to operating in the Arctic (O’Rourke, 2010). Compare these numbers with Finland and Sweden, who each have seven polar icebreakers, Canada with six and the two owned by the U.S., both of which are currently inoperable due to age and mechanical condition (O’Rourke, 2010). Add to the mix the Chinese, who also have an icebreaker, sailing most recently across the Arctic Circle on July 21, 2010 (Xinhua News Agency, 2010). Interestingly, this same ship, the *Xue Long,* surprised the Canadians when it landed at Tuktoyaktuk in 1999 (Teeple, 2010, p. 52). Such activity signals the multinational interest in the region, even by “non-Arctic” nations.

Such political interest was also alluded to in the summary of the 2008 *Arctic Climate Change and Security Policy Conference Report,* which stated:

> Security concerns and issues were not the pressing factor driving Arctic policy. Questions remain however over U.S. and Russian positions and the use of symbolic gestures for political purposes. The government must consider these possibilities as part of the larger strategy...
>
> The Arctic is currently experiencing rapid systemic change with multiple economic, social, political and security implications that are still imprecisely understood. Whether this plays out among the states and parties concerned through international cooperation, or competition and possible conflict is a vital and debated question. (Yalowitz, Collins, & Virginia, 2008, p. 5)

In 2009, RADM David Gove, oceanographer/navigator for the U.S. Navy, recognized the political/military tension and provided his view of national and homeland security interests in the region:

> Competing claims dealing with the Arctic are often political in nature and have important implications. For example, in the summer of 2008 Canada announced that it would increase its military presence in the region, begin construction of a deep-water port on Baffin Island, establish a cold weather training base at Resolute Bay, and build six new ice-hardened ships to patrol the Northwest Passage. During the same period, Russia conducted strategic bomber flights over the area for the first time since the end of the Cold War.
>
> U.S. naval interests will face new challenges in an increasingly ice-free Arctic with a strategic objective to understand potential threats to the United States from the maritime domain. As throughout the global commons, the U.S. Navy must be aware of activities that could be harmful to national security interests in a region that will, no doubt, see fewer barriers to access by potential adversaries in the future. National and homeland security interests pertinent to the U.S. Navy in the region would include early warning/missile defense; maritime presence and security; and freedom of navigation and over-flight. (Gove, 2009)

Figure 4 shows the extent of the 2008 summer transits in the Bering Straits. This data provides insight into the amount of traffic that could lead to national and homeland security interest in the region as described by RADM Gove.

Figure 4. 2008 Bering Straits Transits (From Treadwell, 2009, p. 34)

The political sparring between countries continued in 2010 as noted in the following excerpts from news articles:

> Foreign Affairs Minister Lawrence Cannon on Thursday accused the Russians of "playing games" with a plan to deploy paratroopers to the North Pole this spring." (Canwest News Service, 2010)

> The minister was also sensitive about intelligence reports that suggested the Russians might upstage Canada and other countries vying for a piece of the Arctic by dropping paratroopers at the North Pole in the days or weeks ahead. (Struzik, 2010)

> Russia is interested in joining Chinese developers to exploit oil and gas reserves locked in the Russian section of the Arctic, regional officials said. Dmitry Kobylkin, the governor of the Yamalo-Nenets Autonomous region in the Russian Arctic, expressed interest in a Chinese partnership in oil and gas development during the World Expo 2010 Exhibition in Shanghai. (United Press International, 2010)

These stories and reports are examples of recent political/military tensions; the weight these various claims carry is open for debate. The bottom line is that there is significant multinational political/military interest and capability to operate in the region.

3. Scientific

The level of scientific interest in the Arctic is less debatable. Over 40 research programs, institutions, and organizations exist at the policy and operational levels (National Oceanic and Atmospheric Administration [NOAA], 2010). A number of these are involved in the planning, coordination, and implementation of activities that are carried out in and around Alaska, the U.S. gateway to the Arctic (American Association for the Advancement of Science [AAAS], 2010). This number does not include other political and military organizations that are not conducting research per se but who have interest in the area. In addition, over 4000 Arctic researchers are listed in the Directory at the Arctic Research Consortium of the U.S. (Arctic Research Consortium, 2010).

At the center of the Consortium is the U.S. Arctic Research Commission (USARC), established by Congress under the Arctic Research and Policy Act of 1984. The Commission operates in conjunction with a federal Interagency Arctic Research Policy Committee (IARPC), established under the same legislation. IARPC provides for coordination among federal agencies and works with the Commission to establish an integrated national Arctic research policy. Finally, the Arctic Research Consortium of the United States (ARCUS), established as a not-for-profit corporation in 1988, is intended to serve as a bridge between the advisory bodies such as USARC and IARPC and the organizations that are actually involved in research. This consortium is headquartered in Fairbanks, Alaska (Arctic Research Consortium of the United States [ARCUS], 2010).

4. Increasing Arctic Activity and Potential Scenarios

Figure 5 highlights the fact that nearly 5500 ships transited the Arctic in 2004.

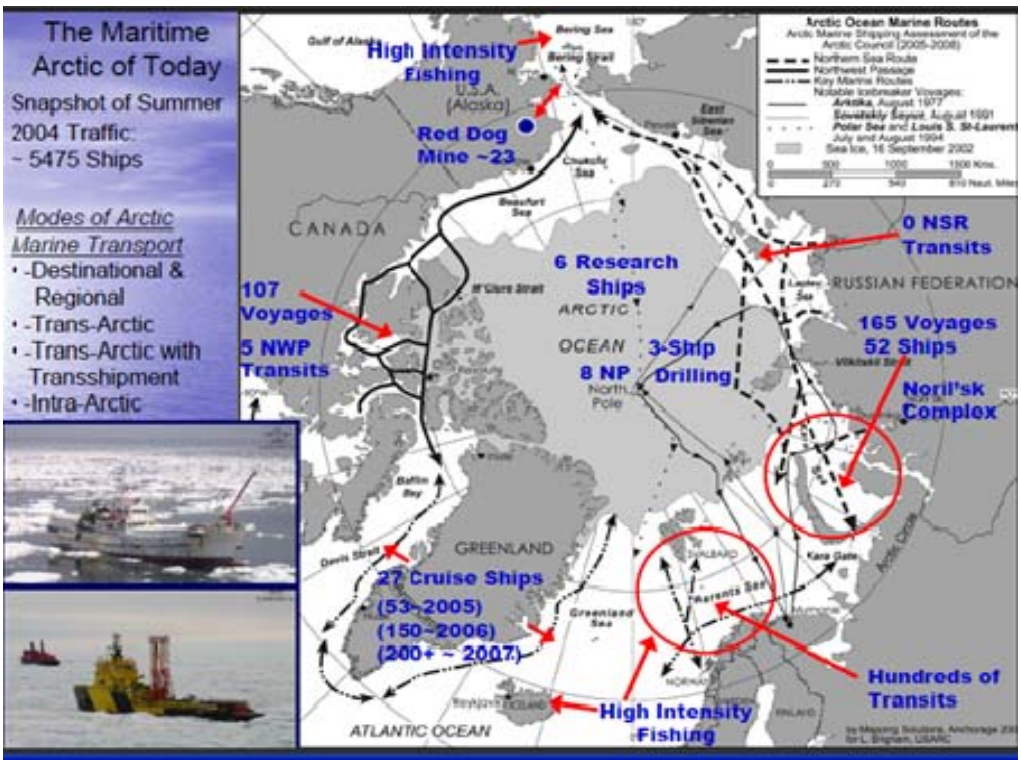

Figure 5. 2004 Arctic Maritime Activity (From Treadwell, 2009, p. 48)

The Arctic Marine Shipping Association (AMSA) reported that same year that the only passenger vessels that traveled in ice-covered waters were the Russian nuclear icebreakers that took tourists to the North Pole, voyages they have been making since 1990 (Arctic Council, 2009, p. 78). This changed in the autumn of 2007, when the first cruise ship tourists sailed from Europe to Barrow, Alaska via the Northwest Passage, which had opened completely for the first time in recorded history (Bryson, 2008). The sudden arrival of 400 German tourists in the northernmost city in the U.S. (Barrow population is 4,054 (State of Alaska, n.d.)) surprised the townspeople as well as the U.S. Coast Guard (Bryson, 2008).

Several different scenarios were possible during this voyage, including the loss of navigation, propulsion and/or need for medical evacuation. More alarming would have been a Titanic situation, such as what happened to the cruise ship EXPLORER in the Antarctic in November 2007 as shown in Figure 6 (Browley &

Revkin, 2007). Luckily, other ships were nearby and all 154 passengers were rescued safely. From a HLS/HD perspective, a rare but thought provoking worst case scenario: the Barrow cruise ship could have brought a potential weapon of mass destruction, or some other dangerous cargo/passengers to shore without detection.

Figure 6. Explorer Stuck in the Antarctic (From *New York Times*, 2007)

The EXPLORER story and different scenarios presented are symbolic of current and future Arctic maritime activity, and the difficulties that coordinating and responding organizations will face. In addition to ferries, fishing vessels, cruise ships and other smaller vessels, the Arctic will host more bulk cargo carriers, oil tankers and liquid natural gas carriers. It is important to note that besides the reduction in ice, there are many events that could increase or decrease potential Arctic traffic, including the safety of other routes, oil prices, major Arctic shipping disasters, transit fees, maritime enforcement, escalation of maritime disputes and the catastrophic loss of the Suez or Panama Canals (Ellis, 2009, p. 15).

The findings from the four-year AMSA project cited another important concern when traffic does increase:

> The current lack of infrastructure in all but a limited number of areas, coupled with the vastness and harsh environment, makes carrying out a response significantly more difficult in the Arctic. Without further investment and development in infrastructure, only a targeted fraction of the potential risk scenarios can be addressed. (Arctic Council, 2009, p. 186)

One scenario, a large environmental disaster, already occurred in an area of Alaska, which is more easily accessed than the Arctic. One of the most expensive in U.S. waters, the 1989 Exxon spill of 10.8 million gallons of crude oil in Valdez cost $2.2 billion and required a massive response effort (Government Accounting Office [GAO], 2007, p. 1). However, what many consider a major event ranks as the thirty-five largest by volume for all spills since 1967 on the list of international tanker spills (GAO, 2007, p. 1). Even if drilling in the Arctic is halted/stymied by the backlash from the latest “Deepwater Horizon” oil spill in the Gulf of Mexico, as long as the demand for petroleum remains, oil tanker traffic could continue to traverse the Arctic via the shorter shipping lanes where response and cleanup challenges are considerably greater.

According to the National Oceanic and Atmospheric Administration, “The 2009 summer minimum [ice] is the third-lowest recorded since 1979. It was 0.6 million km^2 greater than 2008 and 1.0 million km^2 above the record low in 2007” (Menge & Overland, 2009, p. 10). This information indicates that the ability to operate in the Arctic appears to be sustainable at least through the summer months. Some experts believe that, as noted above, “large-scale damage to the Arctic environment from transportation accidents, energy development, fishing, tourism, and the long-range transport of pollutants from the South pose greater immediate threats than classic security issues” (Yalowitz et al., 2008, p. 24). Regardless of the original intent, any increase in human activity could generate homeland defense/security and civil support missions that would require immediate response and/or protection.

5. Summary

While there are various theories regarding climate change causes and precise dates and times of when the Arctic will be ice-free, continued climate change and minimum ice conditions over the past several years suggest that it is not unreasonable to expect increased maritime activity at least during the summer months. These activities will likely include research and exploration expeditions for seabed mapping, natural resource exploration and extraction, and military, commercial and cruise ship traffic. Corresponding to these activities are potential HLS/HD missions including domain awareness, freedom of navigation/mobility, humanitarian assistance, disaster relief, environmental protection and search and rescue. Successfully supporting these missions will depend on a coherent understanding of the activities taking place in the Arctic region. Achieving this level of "situational awareness" will only be possible when all equity partners and stakeholders are sharing relevant information.

In essence, the "status quo" problem is that, from a political, military, scientific and economic perspective, the organizations responsible for supporting homeland defense and security activities in the Arctic are not sharing information in a way that would prevent another event such as the surprise cruise ship arrival at Barrow. Neither is there any sign of unification with regard to roles and responsibilities, where their subject matter expertise converges and diverges, nor how they would mutually support an event occurring today. The current information-sharing landscape is pocketed with expertise, interest, and capability that require a cohesive, interconnected approach in order to leverage the strengths inherent in each of these partners/stakeholders.

For this thesis, the term *equity partner (partners)* is defined as follows*:* organizations responsible for homeland defense and security in the Arctic region (e.g., DHS/USCG, DoD, Department of State (DoS), state of Alaska, local, tribal). Likewise, *stakeholders* are described as "any person, group, or organization that can place a claim on an organization's (or other entity's) attention, resources, or

output or that is affected by that output" (Bryson, 2004, p. 35). In other words, organizations with an interest in the Arctic region that could also contribute to and/or provide information that would support homeland defense and security (e.g., private sector, scientists, researchers, environmentalists, media).

B. RESEARCH QUESTIONS

Is there an existing information-sharing strategy that allows for obtaining, maintaining and providing situational awareness between equity partners and the stakeholders interested in U.S. Arctic region? If not, what information-sharing model might be implemented to support this policy most effectively?

C. HYPOTHESIS

For several years now, rapid climate change has affected the Arctic region. Numerous organizations have an interest in protecting this area and/or ensuring that the region can be explored, remains accessible and safely navigable. A cursory review of some of the likely equity partners and stakeholders (not all are defined in any one comprehensive list) provides insight into the relationship complexities that may have prohibited development of an information-sharing strategy thus far.

For example, at the federal level, since the first Arctic policy, DoS has been engaged as the lead agency in charge of maintaining U.S. interests, including international relationships. While DoS is an important equity partner, it is only one several federal agencies with Arctic interests. As mentioned earlier, DoD and DHS also have specific interests in securing the Arctic. On the other hand, the state of Alaska's widely publicized conflict with the federal government regarding drilling, sea life and other natural resources reveals its economic and political interests in the Arctic region. The same goes for researchers, scientists, and private sector organizations.

The disparity of organizational missions, interests and agendas has not been conducive to development of a naturally occurring information-sharing strategy. Therefore, a community of interest (CoI) needs to be built that focuses on the shared interests of all Arctic region equity partners and stakeholders. This CoI could be successful if: 1) all equity partners and stakeholders can and will contribute/share relevant information; 2) processes and standards will be developed; and 3) a collaborative system for sharing information will be agreed to and adopted by all.

This CoI could leverage one of three existing information-sharing organizational constructs: fusion center (FC), Joint Interagency Coordination Group (JIACG) and Information Sharing and Analysis Center (ISAC). A review of three working models: Alaska Information and Analysis Center (FC AKIAC), US Northern Command's (USNORTHCOM) JIACG, and the ISAC equivalent, Alaska Partnership for Infrastructure Protection (APIP) will be conducted. The model that is significantly better than the other two (based on prescribed criterion) will determine which construct is most suitable to support the new Arctic region policy.

These three models were selected for a variety of reasons/assumptions:

1. The FC (status quo—AKIAC) should be the model of choice based on standards described in national level information-sharing strategies.

2. USNORTHCOM's JIACG is a robust organization that functions at a national level and is also a major partner and therefore should have the capacity/capability/connections to support such an endeavor.

3. The ISAC, emulated by APIP, provides connectivity between many of the local partners/stakeholders and therefore should be competitive in its ability to unite those organizations in order to protect and defend the region.

D. SIGNIFICANCE OF RESEARCH

This research is expected to be significant for the following reasons:

1. Little has been written about this topic because the latest Arctic region policy is quite new. Researchers attempting to understand how the equity partners and stakeholders might leverage one of the standard information-sharing models in support of a national policy may find the study useful.

2. Future research efforts on behalf of other Arctic policy organizations will have insight into developing a practical information-sharing strategy.

3. The immediate consumers for this research will be Alaskan Command/Joint Task Force Alaska, USNORTHCOM, state of Alaska, Alaska Partnership for Infrastructure Protection, Alaska Information Analysis Center and local and tribal organizations.

4. Homeland security practitioners throughout the country looking at alternative information-sharing models for disparate organizations, as well as national level policy and oversight agencies interested in Arctic region policy may find this research useful.

E. METHODOLOGY

The partners with homeland security/defense interests in the Arctic region are disparate organizations at all levels of government. The *National Strategy for Information Sharing* discusses creation of an Information Sharing Environment (ISE) to coordinate information between disparate organizations (National Security Council, 2007). The ISE supports a fusion center (FC) concept intended to be the status quo model for sharing terrorism information between all levels of government and the private sector (National Security Council, 2007). Therefore, such a model should be appropriate for Arctic policy partners.

The policy options analysis methodology is used to compare the status quo (FC) and two other information-sharing models: USNORTHCOM's JIACG and the Alaska Partnership for Infrastructure Protection, which emulates the Information Sharing Analysis Center (ISAC) concept. This methodology will provide insight into which option would be most appropriate to support the information-sharing requirements of the partners/stakeholders supporting Arctic region policy.

This thesis reviews national and departmental level information-sharing strategies to establish a crosswalk between the guidance, requirements and execution expectations. After that, an overview of the history, concepts of operations, guidelines and policies/procedures for each model was conducted. Additional information was discovered regarding the general successes and challenges of implementing and sustaining these three models through reports from the Government Accounting Office, Office of Inspector General, Congressional Research Service and similar official testimony, academic studies and scholarly articles.

The three criteria and scoring method shown below are used to compare the models against each other. The research is then analyzed to determine the extent to which each are met on a scale of low, medium or high, with equal weight applied to each criterion. Comparing the results will determine which model provides the most appropriate construct to facilitate information sharing for Arctic partners/stakeholders.

Table 1. Model Criterion/Comparison

Model Name—Score xx/27 **Level of capability to meet the prescribed criterion.**		
Low/Minimal **Score = 1**	**Medium/Moderate** **Score = 2**	**High** **Score = 3**
1	**2**	**3**
Criterion 1.0 **Robustness:** **Resources, Policies, Political Acceptability**	**Criterion 2.0** **Collaboration:** **Partners, Variety, Frequency**	**Criterion 3.0** **Information-Sharing:** **Systems, Processes, Procedures**
Factors:	*Factors:*	*Factors:*
1.1 Available resources (Personnel, funding, i.e., ability to sustain effort)	2.1 Number of partners (few, some, many)	3.1 Systems used, (Portals/Networks)
Score = x	Score = x	Score = x
1.2 Policies/Guidance (CONOPS, policy manuals, business rules, etc.)	2.2 Levels of Collaboration (Federal/State/Local/Private Sector)	3.2 Processes for information sharing/dissemination (templates, forms, contact lists, databases, etc.)
Score = x	Score = x	Score = x
1.3 Political acceptability (Level of support or opposition)	2.3 Frequency of collaboration (daily, weekly, monthly)	3.3 Standard Operating Procedures (e.g. instructions for collecting and disseminating information)
Score = x	Score = x	Score = x

F. STRUCTURE

Following this introduction, Chapter II will detail a literature review that researches an ongoing information-sharing strategy. Absent such a strategy, Chapter III will provide an overview of the national and organizational information-sharing strategies, enabling an understanding of why, between the myriad of plans, a cohesive information-sharing strategy remains elusive. Chapters IV–VI will review the current models that could potentially serve Arctic region policy partners/stakeholders. Finally, a summary and conclusion are provided in Chapter VII, detailing recommendations for consideration in support of an information-sharing strategy for Arctic region homeland defense and security.

II. LITERATURE REVIEW

An assumption was not made that any one organization is/would be responsible for an Arctic region information-sharing strategy for homeland security/defense. Therefore, this literature review begins with previous policies, defines the participating organizations, and looks for evidence of an existing information-sharing strategy that connects all relevant equity partners/stakeholders.

A. POLICIES

In 1971, the Nixon administration issued National Security Decision Memorandum 144, the first U.S. policy on the Arctic.[1] This policy defined three major areas that the U.S. would support in the Arctic: sound and rational development (minimize adverse effects on the environment), international cooperation, and protecting security interests to include freedom of the seas and airspace (National Security Council, 1971). The memorandum also established an Interagency Arctic Policy Group (IAPG), chaired by the DoS, which included DoD and other appropriate agencies. This group was responsible for implementing, reviewing and coordinating U.S. positions on Arctic interests and programs, with the exception of matters internal to the state of Alaska.

In 1983, the Reagan administration issued National Security Decision Directive 90 as an update to U.S. Arctic policy. This document highlighted the region's growing importance due to "unique and critical interests" related to national defense, resources, energy development, science and environmental protection (National Security Council, 1983). The directive continued the focus on security, development, research and international cooperation. Additionally, the policy directed the IAPG to give priority attention to reviewing potential federal services that may be necessary over the next 10 years, especially those that

[1] Originally classified "SECRET," the policy was declassified May 18, 1977.

impacted agencies with statutory responsibility for search and rescue, enforcing laws/treaties, protecting life, property and the environment. The group was also responsible for "close consultation" with those agencies that were involved domestically.

In 1994, President Clinton issued Presidential Decision Directive/National Security Council 26 (PDD/NSC 26), which, at the time, covered both Arctic and Antarctic Policy (National Security Council, 1994). (Apparently this document was originally For Official Use Only with the Arctic text included. All references to the Arctic have been stripped out of the current PDD/NSC 26 U.S. Antarctica policy that is available as open source material.)[2]

In January 2009, the Bush administration released *Homeland Security Presidential Directive 25 / National Security Presidential Directive 66* (HSPD 25/NSPD 66) *Arctic Region Policy,* which superseded NSC 26 with regard to Arctic policy. Though the words changed slightly, this most recent policy remains consistent with previous policies. This document specifically states that it is U.S. policy to "meet national security and homeland security needs relevant to the Arctic region" (White House, 2009). However, several other priorities also remain: boundary issues (treaties), scientific cooperation, maritime transportation (freedom of the seas), economic/energy, environmental protection and conservation of natural resources. In essence, the same organizations (plus DHS) were listed once more.

B. ORGANIZATIONS/MISSIONS

Four Arctic policies have been in existence since 1971. Since that time, several responsible organizations have connected in various ways to cooperate on diplomatic, social, military, economic, scientific and environmental issues. The latest Arctic region policy also requires a combined effort by multiple agencies in order to achieve the desired outcome. These organizations can be grouped using

[2] This document was not available in the National Security Archives.

a modified diplomatic, informational, military, economic (DIME) principle (the application of national power at all four levels) to determine whether any have developed or are considering an inclusive Arctic information-sharing strategy.

For this review, "DIME" has been modified to "DIMES" as follows:

- *Diplomatic* includes the DoS since the nature of strategic communication with regard to the Arctic has often been handled at the diplomatic level;
- *Informational* mainly considers the media since this group impacts both the public and those organizations seeking to protect/defend the region*;*
- *Military* includes both DoD and DHS since the USCG serves as an important partner in the Arctic area of operations and can be utilized in both capacities*;*
- *Economic* includes environmental, research and private sector organizations, though their subject matter expertise also crosses all boundaries; and
- "*State*" for the state of Alaska, which does not fall into the realm of federal agencies but has significant governmental responsibilities as the gateway to the Arctic for the United States. (Yalowitz et al., 2008, p. 20)

1. Diplomatic

Diplomacy effectively touches upon all areas of the policy at a strategic level: national security, boundary issues (treaties), scientific cooperation, economic/energy, environmental protection and conservation of natural resources. Since the first policy was issued, DoS has been engaged as the lead federal agency in charge of maintaining U.S. interests in Arctic Policy. The DoS also represents the U.S. on the Arctic Council, which is focused mainly on the environment and sustainable development. (The Ottawa Declaration established the council and, at the same time, declared that it "should not deal with matters related to military security" (Department of State, 2010)).

The Arctic Council States address legal issues such as boundaries and Arctic Ocean access through existing institutions. The council has created information-sharing projects and expects those efforts to provide data that will help develop policy, manage communities and inform decision making. Likewise, the council supports the "Sustaining Arctic Observing Networks," which is "a process to support and strengthen the development of multinational engagement for sustained and coordinated pan-Arctic observing and data sharing systems that serve societal needs, particularly related to environmental, social, economic and cultural issues." (Arctic Observing, 2009) The intent of this program is to coordinate a larger network of data sharing; however, security issues are not included in the mission statement.

Though the DoS has instigated these collaborative partnerships, there is no open source evidence that a specific information-sharing capability for Arctic HD or HLS has been constructed or is tied into any of its existing programs. The reason for this may be that DoS needs to be viewed as "neutral" with regard to defense/military activities in order to maintain its diplomatic status.

2. Informational

As alluded to in the introduction, the impact of the media in educating, sensationalizing, persuading, promoting or developing opinions by way of sharing information about the Arctic is without question. However, there is no reason to expect that those included in this group would be leading any type of organized strategy for information-sharing with regard to Arctic security. In this case, the researcher views the media as filling a supporting (or potentially adversarial) role for those responsible for these activities.

3. Military

The latest Arctic policy has generated renewed interest, even though the first U.S. nuclear powered submarine surfaced at the North Pole in the 1950s, long before the 1971 policy was issued. As primarily a maritime domain, the

Arctic has been of interest mainly to the U.S. Navy (USN) and USCG. Many documents have been written about both organizations' respective missions and ability to function in the harsh environment. However, at the government level, little has been published regarding information-sharing with regard to security interests, even though there have been multiple symposia and reports that have dealt with the implications of maritime operations in an ice-free Arctic.

For example, in 2001, the Office of Naval Research and the Arctic Research Commission held a symposium on *Naval Operations in an Ice-free Arctic*. The document provided naval policy changes that would be required to better support Arctic operations in 2015–2020; these did not include a homeland security/defense information-sharing strategy (Office of Naval Research, 2001). In 2007, the "Impact of an Ice-Diminishing Arctic on Naval and Maritime Operations" report was issued by the National Ice Center and Arctic Research Commission.[3] Again, HLS/HD information-sharing was not addressed (National Ice Center, 2007). Finally, in 2009, a third symposium was held. The Center for Naval Analyses provided a briefing on climate change, national security and the impact on naval operations. It also did not mention a strategy for sharing such information (Bowes, 2009).

Similarly, the 2005 *Strategy for Homeland Defense and Civil Support* does not mention the Arctic, though it does describe the need to have:

> …maximum awareness of threats in the approaches as well as the air and maritime interception capabilities necessary to maintain US freedom of action, secure the rights and obligations of the United States, and protect the nation at a safe distance. (DoD, 2005, p. 12)

As well, the 2005 *National Strategy for Maritime Security* (NSMS) acknowledges the Arctic Ocean, but that is the only mention of the word in the

[3] National Ice Center is a multi-agency operational center operated by the U.S. Navy, the National Oceanic and Atmospheric Administration (NOAA) and the U.S. Coast Guard.

entire document (DoD & DHS, 2005). A supporting plan to the NSMS, *National Plan to Achieve Maritime Domain Awareness*, also written in 2005, does not even mention the word "Arctic" (DoD & DHS, 2005).

In the *Draft 2008 U.S. Coast Guard Arctic Strategic Plan*, one of the focus areas is on enhanced homeland security and defense of the Arctic. The document admits that "continued dialogue with the U.S. Navy, USNORTHCOM, Special Operations Command, the intelligence community, and a wide range of federal, state, local, and tribal agencies will be critical..." (USCG, 2008, p. 12). Additionally, "a better understanding of what is occurring on, above, and below the water is a challenge that must be overcome to acquire the actionable intelligence required to successfully prosecute our missions" (USCG, 2008, p. 14). Aside from these instances, the plan generally acknowledges the need to share intelligence and information, but does not describe a process or program devoted to doing so.[4]

At the local level, it is well known that the USCG has already begun testing capabilities, identifying challenges, surveying sea ice and monitoring vessel traffic in U.S. Arctic waters. RADM Gene Brooks, former Commander of Alaska District 17 operations stated:

> Many of the significant threats come from traditional Coast Guard maritime safety and security vectors. Whether the issue is commercial vessel safety, marine environmental protection, living marine resources, or homeland security, the Coast Guard must step forward to protect this emerging domain. (Brooks, 2010)

Neither his speech, nor the USCG brief "The Emerging Arctic: A New Maritime Frontier" mention the need for coordinated information-sharing (USCG, 2010). It is known that the USCG is still studying its role, requirements, and gaps in the Arctic; the results from a "High Latitude Study" are not due until the summer of 2010.

[4] A final version of this document could not be located.

Further review led to several other military authorities that might have interest in developing an Arctic information strategy. USNORTHCOM is responsible for planning, organizing and executing DoD's HD and civil support missions in Alaska. USNORTHCOM shares the maritime HD responsibility in this area with the U.S. Pacific Command (PACOM). Though PACOM's longitudinal boundary is close to Alaska and the command owns maritime assets, none are currently resident to support the Arctic region. USNORTHCOM also has a subordinate, Joint Task Force Alaska (JTF-AK) that has the responsibility for HD missions within the joint operating area, which currently ends at the shoreline.

U.S. Fleet Forces Command (USFFC, Norfolk, VA) is the designated Joint Forces Maritime Component Commander-North for USNORTHCOM and conducts maritime HD throughout the USNORTHCOM area of responsibility. NORTHCOM assigned a formal coordination line between USFFC and JTF-AK. However, the remote location of Alaska and inherent distance from major USN fleet concentration areas make it difficult for USFFC assets to rapidly respond to maritime HD concerns. Based on this current force positioning, local assets from USCG District 17 will likely be called upon as first responders in the Arctic for both HD and HLS missions. To codify this relationship, a memorandum of understanding (MOU) between the JTF-AK Commander and the USCG District 17 Commander was signed on June 23, 2009. The MOU emphasizes coordination to "successfully blend DoD's responsibilities with those of DHS through planning, training, exercises and operations conducted by JTF-Alaska and District 17 officials "…and provides "heightened emphasis on alignment of the two organizations in support of a unified approach to the security and defense of Alaska" (USAF, 2009). The document does not describe information-sharing responsibilities.

In a March 2009 speech, the USNORTHCOM Commander also acknowledged impending Arctic tasks: "In the future, pursuit of natural resources and the potential increase in traffic of northern waterways will demand increased air and maritime surveillance, security, and defense in the Arctic Region"

(Renuart, 2009). He also discussed an evaluation of northern surveillance systems and the ability to monitor the Arctic approaches but did not mention an effort to build an information-sharing strategy. The commander's testimony and the MOU suggest that JTF-AK (under USNORTHCOM) and USCG D17 would be the most likely organizations developing a homeland security/defense information-sharing strategy. Literature relating to such a strategy was not discovered during this review.

4. Economic/Environmental

A great deal of the literature dedicated to climate change and its affect on the Arctic has focused on private sector economic and environmental issues. As mentioned in the introduction, the oil industry has a vested interest in the Arctic. In fact, the state of Alaska's two largest taxpayers are BP and ConocoPhillips (Conoco Phillips, 2006). (The two companies stated that in 2006, the oil industry generated about 34,000 jobs and around $4.4 billion in Alaska payroll, roughly 20 percent of the private sector (Conoco Phillips, 2006)). The oil industry spends more than two billion dollars per year on goods and services within the state, roughly equal to the state's general fund budget spending (Conoco Phillips, 2006). The significance of this lens on the Arctic and subsequent volume of writing that is dedicated to these economic concerns is readily apparent.

Similarly, the Arctic Marine Shipping Assessment 2009 Report provides insight into the spotlight on environmental issues:

> …more than 185 experts participated directly in the work of the AMSA. Thirteen major AMSA workshops were held from July 2006 through October 2008 on a broad range of relevant topics, including scenarios of future Arctic navigation, indigenous marine use, Arctic marine incidents, environmental impacts, marine infrastructure, Arctic marine technology and the future of the Northern Sea Route and adjacent seas. (Arctic Council, 2009, p. 3)

Other stakeholders agree that the environment and management of natural resources are the most pressing security issues in the North (Yalowitz et al., 2008, p. 22). From an information-sharing standpoint, there are over 40 research programs, institutions, and educational organizations (including a University of the Arctic) conferring at the policy and operational level (NOAA, 2010). Many of these organizations have been monitoring and reporting on the various environmental aspects of the Arctic for decades, some with security interests.

One example, the Institute of the North (founded in 1994), is a:

> …center for the study of commonly owned lands, seas and resources using the 'owner state' of Alaska as a model. Its mission combines both economic relevance and geopolitical urgency as most trouble spots around the world are found in regions where the commons has been mismanaged or exploited. (Institute of the North, 2010)

Within this organization is the Security and Defense Program, which "conducts research and educates policymakers on strategic issues relating to the defense of the United States that particularly concern decision makers in Alaska and at the state and local level throughout the nation" (Institute of the North, 2010). The program publishes a newsletter entitled "Vanguard," which provides synopsis information of various topics including missile defense, homeland security, cyber security and wire releases on current events (Institute of the North, 2010). Similarly, there is an Alaskan sub-cabinet that cooperates on issues involving interested stakeholders such as the University of Alaska, scientists, non-governmental organizations, the state of Alaska, federal government authorities and indigenous group leaders (Yalowitz et al., 2008, p. 23).

The volume of information generated by this sector has been focused historically, on economic, scientific, environmental and educational areas. While these organizations are certainly contributors of information that would support

Arctic homeland defense and security, they do not appear to have developed a homeland security/defense information-sharing strategy.

5. State of Alaska

The state of Alaska is the U.S. gateway to the Arctic region. The Division of Homeland Security and Emergency Management (DHS&EM) was created by Alaska Statute 26.20.025 (Alaska Legal Resource Center, 2010). Subsequently, Administrative Order No. 203, issued January 13, 2003, placed the state DHS within the Department of Military and Veterans Affairs (DMVA) to “maximize the security of the citizens of Alaska” (State of Alaska, 2004). The state DHS is the:

> …single, statewide focal point for coordinating the State's efforts to prevent terrorist attacks, reduce Alaska's vulnerability to terrorism, and minimize the loss of life or damage to critical infrastructure, and recover from attacks if they occur. (State of Alaska, 2010)

One of the duties of DH&EM is to coordinate federal, state, local, and private agencies' homeland security activities. They also coordinate the state homeland security strategy/plan with the state emergency plan and with the homeland security and disaster plans of the federal government. In addition, the organization provides other planning, prevention, preparedness, response and mitigation measures designed to eliminate or reduce the threat or effect of an attack.

The 2009 Alaska State Homeland Security Strategy (AKHSS) recognizes the importance of reducing vulnerabilities to terrorist attacks, major disasters and emergencies. It acknowledges that this will require coordination, cooperation and a focused effort throughout federal (military and civilian) and state agencies, local jurisdictions, tribal, private and non–profit organizations (State of Alaska, 2009, p. 1). Homeland security grant dollars for DHS&EM in fiscal year 2009 totaled six point five million dollars (DHS, 2010). These funds were allocated to provide for critical tasks at the state level that include crisis management, intelligence

gathering/notification and critical infrastructure analysis (Office of Management and Budget, 2010). A further review of the 2008 and 2009 AKHSS revealed three goals relative to information sharing:

Table 2. Comparison of 2008 and 2009 AKSHSS Information-sharing Goals

2008 AKSHSS	**2009 AKSHSS**
Goal 2: "strengthen information and intelligence sharing"	Goal 4 is identical (State of Alaska, 2009, p. 15)
Goal 2—Objective 2A: "develop a network and procedures among local, tribal, State and Federal agencies, and private sector organizations for the dissemination of critical, time-sensitive intelligence among participants." (State of Alaska, 2008, p. 11)	Goal 4—Objective 4A is identical (State of Alaska, 2009, p. 15)
Goal 2—Objective 2A—Step 2: "analyze the integration of existing interagency information-sharing processes into a statewide fusion center." (State of Alaska, 2008, p. 11)	Goal 4—Objective 4A—Step 2: "analyze the integration of existing interagency information-sharing processes into a virtual statewide fusion center. (State of Alaska, 2009, p. 15)
Goal 2—Objective 2A—Step 3: "develop a concept plan for HSIN State portal and implement recommendations." (State of Alaska, 2008, p. 11)	Goal 4—Objective 4A—Step 3:"continue to expand the use of the HSIN State portal to include expansion to the Homeland Security Data Network..." (State of Alaska, 2009, p. 15)

The verbiage in these documents indicates that an information-sharing strategy is not yet firmly in place. Given the fact that neither the 2008 nor 2009 strategies mention the word "Arctic," it can reasonably be assumed that a specific strategy for information-sharing focused on that topic also does not exist.[5] (The capabilities and status of the fusion center will be covered further in Chapter IV.)

One final note: in August 20, 2009 the governor of Alaska gave a policy speech on the strategic importance of the Arctic before the U.S. Senate Subcommittee on Homeland Security Appropriations (Parnell, 2009). He acknowledged the importance of national and homeland security with respect to

[5] The 2008 and 2009 AKHSS documents are nearly identical in verbiage with regard to vision, mission and goals.

protecting the Arctic, but his message did not include the words “information sharing” (Parnell, 2009). He mentioned the development of a “National Arctic Doctrine” that includes all stakeholders, but did not elaborate on what this effort entailed (Parnell, 2009).

C. CONCLUSION

A variety of Arctic policies have been in existence since 1971. Since that time, several responsible organizations have connected in various ways to cooperate on diplomatic, social, military, economic, scientific and environmental concerns. These organizations were grouped using a modified “DIMES” approach to determine whether any had developed or were considering an Arctic information-sharing strategy focused on homeland security/defense. This literature review indicates that while there are many agencies involved in supporting Arctic Policy, and some have developed a considerable willingness and capability to share information, so far, there is no publicly advertised system that is collecting and sharing homeland security/defense information between all Arctic policy partners/stakeholders.

A 2009 draft report submitted to the state of Alaska confirms this conclusion from a research perspective:

> There is no single agency, organization, or collaborative association within Alaska that is tasked with systematically coordinating the identification, collection, compilation, analysis, and publishing of climate change data and research. This important task is required to ensure the quality necessary to effectively support decision-making and evaluate and manage multifaceted risks and threats such as those associated with climate change in Alaska. (State of Alaska, 2009, p. 5)

The next chapter will inform the reader as to why the three information-sharing models have been selected for review.

III OVERVIEW—INFORMATION-SHARING STRATEGIES

This chapter provides a snapshot of six information-sharing strategies that affect the majority of the responsible Arctic region partners (homeland security, intelligence, law enforcement and defense). The overarching *National Strategy for Information Sharing* is reviewed first in order to lay the foundation for the status quo/option one (fusion center) and policy option two (information sharing analysis center). The next four strategies, DHS, Intelligence Community (IC), Department of Justice (DoJ) and Federal Bureau of Investigation (FBI) provide background information and highlight interagency linkages and common ties between the organizations. The *DoD Information Sharing Strategy* is also covered as a lead-in to the third policy option, the *Joint Interagency Coordination Group* model. Finally, a description and highlights of the "Information Sharing Environment," the entity intended to provide a shared information space, common standards, best practices and accountability for the entire community supporting terrorism information sharing, is also provided.

The intent of this overview chapter is threefold: 1) communicate the basic principles of each document, 2) relate the extent to which the documents converge on an existing implementable construct for Arctic policy partners, and 3) provide insight into why the status quo and two option model constructs were selected for review. Instead of citing the applicability of each strategy to the Arctic policy partners, a general recap of the strategies is provided at the end of the chapter.

A. NATIONAL STRATEGY FOR INFORMATION SHARING (NSIS)

The overarching guidance for sharing information between the public and private sectors comes from the 2007 NSIS, which describes both a strategic vision and guiding principles in one document. This strategy acknowledges that homeland security and law enforcement information related to terrorism "can come from multiple sources at all levels of government as well as the private

sector organizations and foreign sources" (National Security Council, 2007, p. 1). It further describes that such information is needed to support efforts to prevent terrorist attacks, develop critical infrastructure protection and resilience plans, and prioritize emergency management response and recovery planning activities (National Security Council, 2007, p. 1).

The NSIS takes its lead from the 2006 *National Security Strategy* and is aligned with other strategies such as *Homeland Security* and *Combating Terrorism* (National Security Council, 2007, p. 5). The document cites the 2004 Executive Order (EO) 13354 that created the National Counterterrorism Center (NCTC), a clearinghouse for terrorism intelligence and information sharing between DOJ, DHS and other appropriate agencies. All federal agencies are slated to provide information to the NCTC, which is the "Federal fusion center" that analyses and integrates all terrorism related intelligence (National Security Council, 2007, p. 15). Inside the NCTC is the Interagency Threat Assessment Coordination Group (ITACG), which in turn disseminates terrorism related information products to state, local, tribal and private sector partners. ITACG is intended to be the link between the Intelligence Community, DHS, FBI state and local representatives until the ISE is mature (National Security Council, 2007, p. 18).

The NSIS frequently refers to the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). IRTPA created the *Information Sharing Environment* (ISE), to "enable trusted partnerships among all levels of government, private sector and foreign partners in order to more effectively detect, prevent, disrupt, preempt and mitigate the effects of terrorism in the United States" (National Security Council, 2007, p. 10). The ISE is designed to break down existing stovepipes and extend common standards to state, local and tribal governments and the private sector, enabling full partnership participation. This entity will be covered more thoroughly in a subsequent section.

1. Fusion Centers

The NSIS describes support for establishing a network of state and major area fusion centers. The document acknowledges that fusion centers "will serve as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" (National Security Council, 2007, p. 20). Fusion centers are, therefore, intended to be the conduit for information sharing to and from the federal government; they may also further customize the information received from federal agencies for their own use. Guidelines and baseline capabilities for fusion centers were developed through the *Global Justice Information Sharing Initiative* and the Homeland Security Advisory Council.

The intent is for fusion centers to become interconnected with the federal government and each other. The NSIS acknowledges that "the Federal government will support the establishment of these centers and help sustain them through grant funding, technical assistance, and training..." (National Security Council, 2007, p. 20). The goal is to have federal government personnel imbedded within fusion centers where possible. At the same time, the federal government expects that "locally generated information that is not threat or incident related is also to be gathered, processed, analyzed and interpreted by those same fusion centers in coordination with locally based Federal officials and then further disseminated to the national level..." (National Security Council, 2007, p. 20). This could be interpreted as an "all-hazards" approach, requiring fusion centers to provide more than just law enforcement/terrorism information collection and dissemination. This is an important point for Arctic policy partners since gaining situational awareness in the region would require a variety (all source) of information.

Due to the mandate described above, the *Alaska Information Analysis Center (*the "fusion center" for the state of Alaska and Arctic partner) will be reviewed in Chapter IV as the "status quo" option. (The name for the Alaska fusion center should not be confused with the Information Sharing and Analysis Center construct covered in the following paragraph.)

2. Information Sharing and Analysis Centers (ISAC)

The NSIS acknowledges that 85 percent of the infrastructure and resources critical to the nation is in the hands of the private sector, which has made significant investments with regard to interagency information sharing (National Security Council, 2007, p. 4). (Much of this effort stemmed from the 1998 Presidential Decision Directive/National Security Council-63 *Critical Infrastructure Protection*, which called for the creation of ISACs. Multiple ISAC organizations have since expanded across the various infrastructure sectors.)

The NSIS recognizes that industry plays a significant role in building an effective two-way information flow between public and private sectors, and it expects that information from critical infrastructure and key resource owners will be incorporated into the integrated network of state and major urban area fusion centers. The strategy also emphasizes that the ISE is slated to expand these original information-sharing mechanisms by adding secure networks that will encourage more collaboration between the public and private sectors (National Security Council, 2007, p. 10).

The NSIS also recognizes that many private sector organizations currently leverage both ISACs and fusion centers. For this reason, the researcher chose to review the Alaska Partnership for Infrastructure Protection (Chapter VI), which emulates the ISAC construct. Many of the Arctic policy partners are already members of this organization; they connect daily on issues related to homeland security as well as all-hazards within the state of Alaska.

In summary, the NSIS does not dictate a single national model for information sharing that Arctic stakeholders' can readily apply. It simply lays out a foundation, including several organizations intended to promote/facilitate information sharing with the federal government.

B. DHS—INFORMATION SHARING STRATEGY (DHS ISS)

This 2008 document refers to the expectation of the President and Congress for DHS to "play a central role in augmenting the Nation's ability to gather, analyze and disseminate information and intelligence" (DHS, 2008, p. 2). The strategy states that the IRTPA and other regulatory documents ensure that DHS would have an essential part in the ISE. It describes a close relationship with the Program Manager (PM) ISE in order to "coordinate the development of a common National framework for information sharing" (DHS, 2008, p. 3). The strategy recognizes that "clearly defined institutionalized rules, roles and responsibilities are necessary to ensure effective information sharing" (DHS, 2008, p. 6). The objectives stipulated in the strategy include: the need for integrating fusion centers, coordinating with the ISE, recognizing the needs of other organizations and integrating those needs as part of the DHS ISE, and ensuring that DHS technology platforms facilitate information sharing with partners.

The DHS ISS cites the need to coordinate trusted information-sharing policies within the ISE framework based on known community needs, while exchanging information with non-federal partners using an inclusive, networked fusion center construct. The document specifically states, "information needs and missions of all stakeholders, not technology, will drive the design of the DHS information sharing environment. Technology will be used to enhance and simplify information sharing" (DHS, 2008, p. 7). In other words, tools will be used in support of protocols that facilitate interoperability, allowing cross-functional information sharing between communities of interest.

C. INTELLIGENCE COMMUNITY—INFORMATION SHARING STRATEGY (IC ISS)

This document was also issued in 2008 and likewise states that the President and Congress mandated a more integrated enterprise for routine intelligence community information sharing. It cites many of the same authorities: IRTPA, EO's, and the 9-11 Commission, as catalysts for developing the strategy. The IC ISS recognizes the progress that has been made due to the standup of the NCTC, ISE, and related partnership efforts. However, "these endeavors, though proving to be excellent in facilitating greater information sharing, are the 'tip of the iceberg' and continued focus on 'accelerated information sharing' is needed" (U.S. Intelligence Community [IC], 2008, p. 3). There is mention that information sharing is a behavior not technology, and such behavior means: "exchanging intelligence information between collectors, analysts and end users in order to improve national and homeland security" (IC, 2008, p. 3). The new information-sharing model is shown in Figure 7.

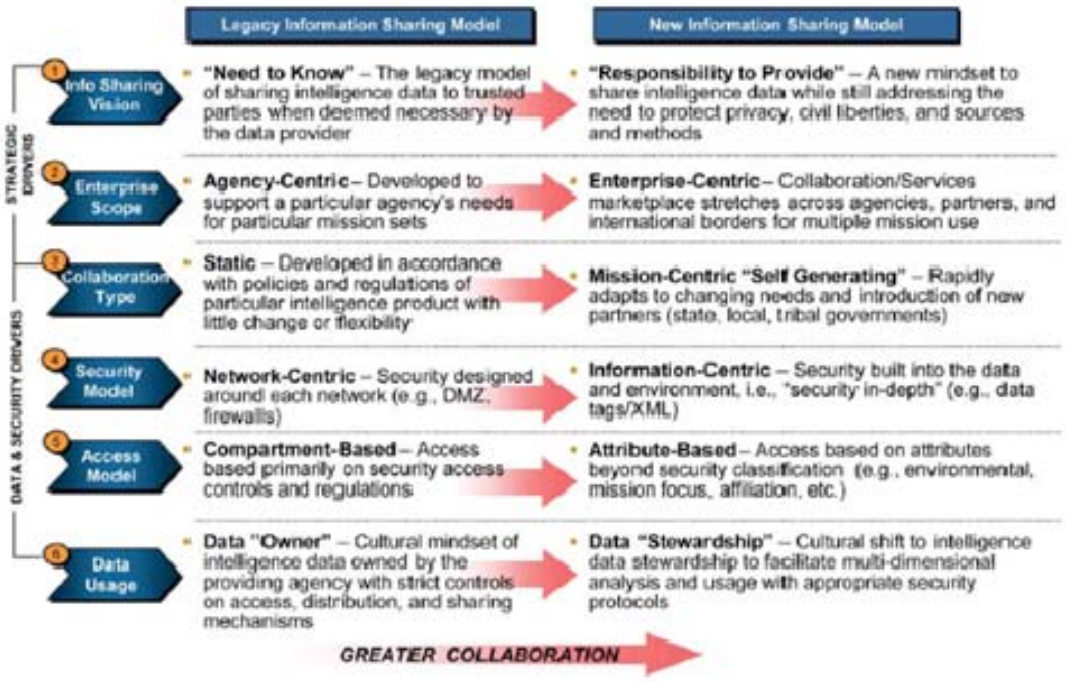

Figure 7. USIC ISS Information Sharing Model (From IC ISS, p. 9)

The IC ISS also references the changing threat environment for national and homeland security customers and how these emerging threats require intelligence from various sources. It acknowledges that the old business model does not satisfy modern requirements: “...in today's environment the traditional lines between foreign and domestic, and strategic and tactical intelligence operations, and customer and producer are blurring, creating an imperative to improve integration between National and Departmental intelligence programs” (IC, 2008, p. 7). This will be accomplished via an integrated intelligence enterprise.

The new IC ISS information-sharing model discusses a “responsibility to provide” where the “end-state is a common trust and information environment, wherein all intelligence information is discoverable and mission accessible...Ultimately, the new information-sharing model will foster greater collaboration among intelligence community stakeholders and partners” (IC, 2008, p. 9). The IC ISS also promotes five keystones: these include: maximizing the availability of information retrieval and dissemination; discoverability and accessibility; trust and understanding of missions; a culture that rewards information sharing; and a single information environment that will enable improved information sharing (IC, 2008, p. 10).

The goals supporting these keystones are similar to the other strategies: uniform information sharing, policy and governance; universal information discovery and retrieval; a common trust environment and enhancing collaboration across the community. The goals are fleshed out with actions that develop policies, processes, procedures, standards and tools including virtual collaboration, identity management and information security policies using a risk management approach to protect sources and methods. The implementation strategy for these efforts consists of five building blocks: governance, policy, technology, culture and economics (IC, 2008, p. 17). These keystones, goals, and building blocks are very comparable with the strategies discussed earlier.

There are also references to aligning with other information-sharing efforts such as the NSIS, which the document concludes “will improve interagency at the Federal level, while building information sharing bridges between the Federal Government and our non-Federal partners” (IC, 2008, p. 17). The IC ISS notes that leveraging the ISE and DHS ISS will “ensure alignment to the overarching community-wide goals and objectives for information sharing” (IC, 2008, p. 17). The document made no direct reference to fusion centers, labeled the ISE as the solution for information-sharing requirements, and touted the NCTC as integrating “all intelligence possessed or acquired by the U.S. government pertaining to terrorism and counterterrorism and for ensuring that agencies have access to and receive intelligence needed to accomplish their activities” (IC, 2008, p. 17). In essence, this strategy focuses inwardly on how the IC will comply with the NSIS and provided consensus with regard to the ISE as the place to share.

D. DEPARTMENT OF JUSTICE (DOJ) LAW ENFORCEMENT INFORMATION SHARING PROGRAM (LEISP)

While somewhat dated, this 2005 document remains DOJ’s transformation document on how it will share law enforcement information with all partners. The vision is to “create relationships and methods that allow information to be shared routinely across jurisdictional boundaries to prevent terrorism...” (U.S. Department of Justice [DoJ], 2005, p. iii).The intent is to achieve this vision by “formulating information sharing policies and standard business practices and by creating a unified, Department-wide technology architecture that will position DOJ as a committed partner in the information sharing environment of federal, state, local, and tribal law enforcement agencies” (DoJ, 2005, p. iii). This strategy guides all DoJ information sharing with the ISE and “contributes to the fulfillment of the ISE by providing a single point of contact for DoJ information and by providing a foundation for information sharing among law enforcement at the federal, state, local, and tribal levels” (DoJ, 2005, p. 6). The document also addresses the “move from a culture of ‘need to know’ towards a culture of ‘need

to share' in which information is shared as a matter standing operating procedure" (DoJ, 2005, p. iii). The LEISP describes three tracks that expect to provide a "single face" with partners: leveraging existing technology, building new platforms, and enhancing national level interconnectivity. These are similar goals to those expressed in previously covered strategies (DoJ, 2005, p. iii).

LEISP also provides:

> …uniform DOJ policies and processes for sharing its information....a foundation for broadening the reach of the ISE to the thousands of state, local, and tribal law enforcement partners, where the process of transforming data to information and finally to intelligence is most critical. (DoJ, 2005, p. 6)

This document makes it clear that law enforcement information is more than the IRTPA focus on terrorism information sharing. The strategy is focused on collecting all law enforcement information and creating a "one DOJ" approach to sharing. Nearly the same vintage as the NSIS, the LEISP points to the ISE as the connective entity and mentions the ongoing development and eventual connection to the fusion centers.

E. FEDERAL BUREAU OF INVESTIGATION (FBI) NATIONAL INFORMATION SHARING STRATEGY (FBI NISS)

The 2008 NISS was selected for review due to its currency and the FBI's key role in terrorism information sharing for Arctic policy partners. This strategy falls under the umbrella of the LEISP; both indicate a strong connection to the ISE. The NISS provides a now familiar vision, goals and framework for information sharing with partners at all levels of government, the private sector and foreign partners. It also "addresses the cultural and technological changes required to move the FBI to a 'responsibility to provide culture'" (FBI, 2008). Similar to the preceding strategies, this policy distinguishes the framing documents (IRTPA, EO's, LEISP, ICISS, NSIS and ISE) as mandates and guidance. The NISS has two primary objectives: creating a culture of information sharing and developing and maintaining an information technology platform that

will support relevant activities. The document highlights five categories of information-sharing customers: 1) presidential offices, 2) DoJ and other federal agencies, 3) state, local, tribal, 4) private sector and 5) foreign partners (FBI, 2008).

The NISS references a myriad of “information sharing entities” that the FBI will interface with at the national level, for example: NCTC, Terrorist Screening Center, Terrorist Explosive Device Analytical Center, National Gang Intelligence Center and National Crime Information Center (FBI, 2008). The document relates that the NSIS mandated the use of the ISE for information sharing with state, local, and tribal entities, and that those efforts include: state and major urban area fusion centers, e-Guardian and the ITACG (FBI, 2008). At the private sector level, the FBI will interface with InfraGard, Cyber Initiative Resource Fusion Unit and the Domestic Security Alliance Council (FBI, 2008).

In summary, the DHS, IC, DoJ and FBI strategies indicate commonalities in the way they support the NSIS, alluding to the variety of organizations that also process homeland security information. The connection between these strategies and the ISE will be covered later in this chapter.

F. DEPARTMENT OF DEFENSE INFORMATION SHARING STRATEGY (DOD ISS)

The 2007 DoD ISS was prepared by the Information Sharing Executive, Office of the Chief Information Officer. The document defines information sharing as “making information available to participants (people, processes, systems)” and “cultural, managerial and technical behaviors by which one participant leverages information held or created by another partner” (Department of Defense [DoD], 2007, p. 16). The document acknowledges the NSIS, EO 13388 and IRTPA, promoting that “the strategy and efforts must be synchronized in order to achieve the unity of effort as well as economic and operational efficiency” (DoD, 2007, p. iii). The strategy promotes a common vision to synchronize initiatives to share information among DoD components,

international coalition partners, and the private sector.[6] The vision acknowledges that individual or limited approaches will not ensure success among the agencies and that trust and agreed upon rules must be dominant factors. The DoD ISS looks to achieve its goals by promoting a "federated information sharing community and environment to maintain trust, promote collaboration, leverage information integrators in the community and reduce the seams between organizations"[7] (DoD, 2007, p. 10).

The strategy confirms that DoD intends to continue working inside the "evolving Federal approach" and acknowledges that external agencies may have different operating environments that should not preclude successful information sharing (DoD, 2007, p. 2). Likewise, it stresses that:

> …the Department must have the ability to transfer information to and obtain information from external partners, overcoming situations where these partners may have disparate processes and capabilities and whose role and nature may not be known prior to an event. (DoD, 2007, p. 4)

It also acknowledges that DoD has to adjust to "a major cultural shift ...from information ownership to information stewardship" (DoD, 2007, p. 10). The document highlights five touchstones of successful information sharing: culture, policy, governance, economic, and resources in technology and infrastructure as shown in Figure 8. The strategy recognizes that "effective information sharing enables DoD to achieve dynamic situational awareness and enhance decision-making to promote unity of effort across the department and with external partners" (DoD, 2007, p. 2).

[6] Partner: an entity that takes part in an information sharing activity with DoD (DoD, 2007, p. 16).

[7] Collaboration: pattern of interaction where two or more parties are working together toward a common purpose (DoD, 2007, p. 16).

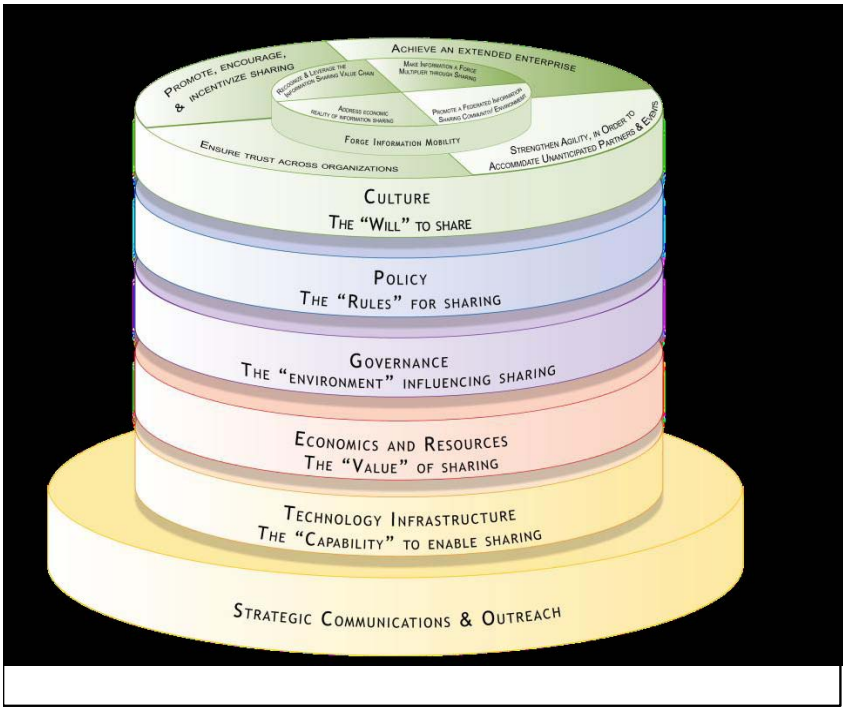

Figure 8. Information Sharing Implementation Touchstones (From DoD, 2007, p. 10)

The DoD ISS argues that synchronizing across information-sharing initiatives "will give the DoD flexibility to share information with planned and unanticipated partners across planned and unanticipated events" (DoD, 2007, p. 15). At the same time, "the department will seek opportunities to reach out to partner organizations that may benefit from this information sharing initiative" (DoD, 2007, p. 15).

In February 2009, DoD issued Directive 8000.01 on *Management of the Department of Defense Information Enterprise*. This document "provides direction for information sharing among all DOD components and mission partners, consistent with the National Strategy for Information Sharing" (DoD, 2009, p. 1). The policy is:

> ...that information shall be considered a strategic asset to the Department of Defense; it shall be appropriately secured, shared,

> and made available throughout the information life cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy." (DoD, 2009, p. 2)

The glossary states that the DoD information enterprise shares "information across the Department of Defense and with mission partners" (DoD, 2009, p. 16).

The Directive was followed shortly thereafter by the April 2009 *Information Sharing Implementation Plan*, issued by the DoD Office of the Assistant Secretary of Defense for Networks and Information Integration / Chief Information Officer. Under focus Area 10, *Supporting DoD's Mission Needs Across Federal Information Sharing Initiatives,* during fiscal year 2010–2014 several tasks and responsibilities are highlighted. These include: "appropriate" support for development of the "Federal ISE" and "determine the level of DoD engagement and support" for the Interagency Threat Assessment Coordination Group, state and major urban area fusion centers and developing "DoD's portion of the Federal ISE Shared Space" (DoD, 2009, p. 26). These statements indicate that DoD is still determining the level of engagement and support for both the ISE and fusion centers.

This researcher believes that the intent of the DoD ISS, Directive 8000.01 and Information Sharing Implementation Plan is to share information with other organizations in accordance with the NSIS, while allowing DoD the autonomy to develop its own information enterprise and subordinate coordination groups responsible for interagency information sharing. Accordingly, Chapter VI provides a review of USNORTHCOM's JIACG, the likely organization that would be responsible for homeland defense information sharing with Arctic policy partners.

G. INFORMATION SHARING ENVIRONMENT (ISE)

While the NSIS provides the overarching guidance stipulating information sharing, the ISE is intended to be the framework for connecting participants. This means coordination among all levels, sharing intelligence products and enabling

State, local and tribal government to gather, process, analyze and share information (National Security Council, 2007, p. 11). In other words, the ISE could be thought of as the Web intended to facilitate linkage between all participants of the information-sharing communities, which includes Arctic policy partners. Figure 9 diagrams the intended interaction. It is important to review the status of this entity in order to understand the role it plays with regard to an existing, usable information-sharing construct.

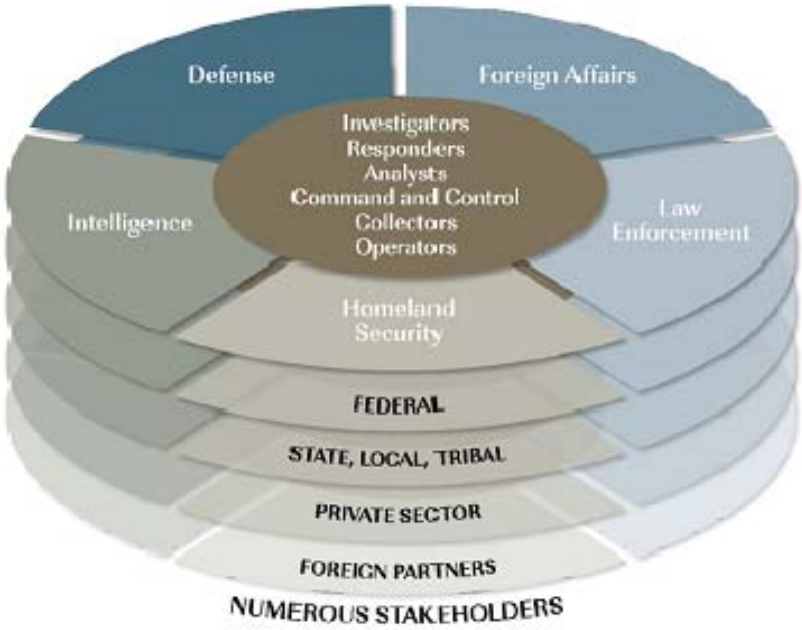

Figure 9. The ISE (From McNamara, 2009, p. 3)

As mentioned in the NSIS, Section 1016 of the 2004 IRTPA called for the ISE and defined it as an approach that facilitates the sharing of terrorism information (National Security Council, 2007, p. 12). Recall that the NSIS referenced the 2004 EO 13356, which established an Information Systems Council and dictated that agency heads would create common standards and share/disseminate information to the greatest extent allowable by law.

EO 13356 was superseded by EO 13388 in October 2005, including the new Director of National Intelligence and a name change from Information Systems to Information Sharing Council (ISC). (These EOs were designed to

ensure the proper coordination of federal departments and agencies participating in the ISE.) The ISC is chaired by the Program Manager (PM) and includes many of the Arctic partners: Secretaries of State, Defense, Homeland Security, and Directors of National Intelligence, CIA, FBI and NCTC (National Security Council, 2007, p. 12).

The PM and ISC are required to "develop policies, procedures, guidelines, and standards, and proper coordination among Federal departments and agencies participating in the ISE" (National Security Council, 2007, p. 12). The Implementation Plan was designed to build:

> …a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States by the effective and efficient sharing of terrorism and homeland security information. (National Security Council, 2007, p. 10)

The intent of the ISE is to: create a culture of sharing, reduce barriers to sharing, improve sharing practices with all partners (federal, state, local, tribal and foreign), and institutionalize sharing[8] (National Security Council, 2007, p. 10).

The 2005 *Preliminary Report on the Creation of the Information Sharing Environment* (due six months after enactment of the IRTPA) described initial technical, legal and policy issues brought forward by the ISC via the Program Manager—Information Sharing Environment (PM-ISE). Three of the five issues presented concerned ambiguous and conflicting authorities and policies governing agency roles and responsibilities, lack of organizational trust, and the ability to collaborate timely due to limited access to information (Russack, 2005, p. 4). The following year, the new PM-ISE stated:

[8] "The term 'information sharing' in the ISE context means that the proper information, properly controlled, gets to the right people in time to counter terrorist threats to our people and institutions" (Paul, 2010, p. 1).

> I believe that right now the main problem is not too little information flow from the five federal community members to State and Local elements, but too much flow of uncoordinated information to State and Local levels...In contrast there is little information flow from local and tribal levels the state and federal level. (McNamara, 2006, p. 4)

During this same time, the PM highlighted success stories, including the NCTC, Terror Screening Center, fusion centers, DHS's Web portals, DOJ's LEISP and DoD's Global Information Grid, which was developed in concert with the ODNI IC Enterprise Architecture "to support all DoD, National Security, and related IC mission and functions in war and peace" (McNamara, 2006, p. 7). It should be noted that when mentioning fusion centers he added:

> There is, however, no national strategy that defines federal collaboration with these centers. Each State and Local fusion center has developed its own way of interfacing with various federal agencies entities involved in terrorism prevention and response efforts. Additionally, fusion centers rely on multiple channels to exchange terrorism information with the various Federal entities involved in investigatory, prevention, response, and recovery activities. It is one of my highest priorities to greatly improve this situation. (McNamara, 2006, p. 10)

The PM's statement also provided guiding principles for the ISE effort at that time, which included: common standards and best practices, information access via a shared information space, security and privacy safeguards, risk management for information disclosure, trust built through auditing, performance evaluation, accountability and transparency (McNamara, 2006, p. 14).

Another of these principles was the deployment of a "decentralized, distributed and coordinated model so that the handling of terrorism information in the ISE will take place directly among users, using a Web-enabled, network model accessible to each of the stakeholders in information sharing" (McNamara, 2006, p. 13). This has apparently evolved into the current approach within the 2008 ISE Enterprise Architecture Framework which intends to: "leverage existing information sharing policies, business processes, technologies, systems, and

promote a culture of information sharing through increased collaboration" (McNamara, 2008, p. 11.) Figure 10 highlights the framework as described.

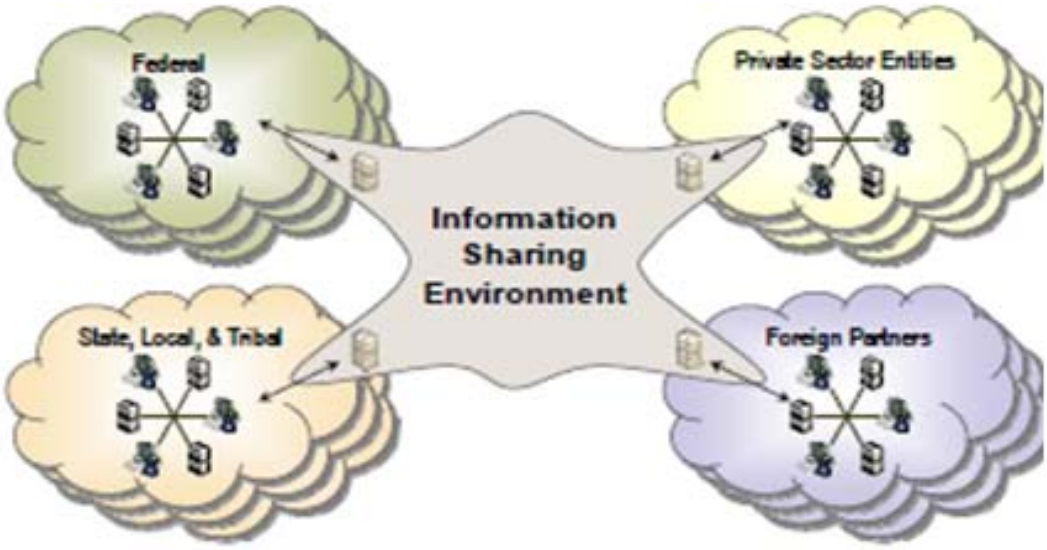

Figure 10. ISE Framework (From Enterprise Architecture Framework Version 2.0, 2008 p.12)

The ISE Enterprise Architecture Framework also provides that:

> ...while participants in the ISE are still responsible for their own counterterrorism missions and systems supporting these missions, the physical ISE, as a functioning system-of-systems, will improve the overall effectiveness of individual counterterrorism business processes and capabilities through increased access to terrorism information across the ISE community. (McNamara, 2008, p. x)

Fast forward three years to the *Third Annual Report to the Congress on the ISE Progress and Plans* in 2009. The original four goals are restated: culture of sharing, reduce barriers, improve sharing practices with federal, state, local, tribal and foreign partners and institutionalize sharing (McNamara, 2009, p. vii). A new framework is presented that "creates critical linkages between the four primary and enduring ISE goals, fourteen sub-goals, and a resulting set of outcomes, objectives, products, activities, and associated performance

measures" (McNamara, 2009, p. 32). Aligned to the framework is the new ISE Maturity Model, shown in Figure 11, which is intended to assess progress against goals.

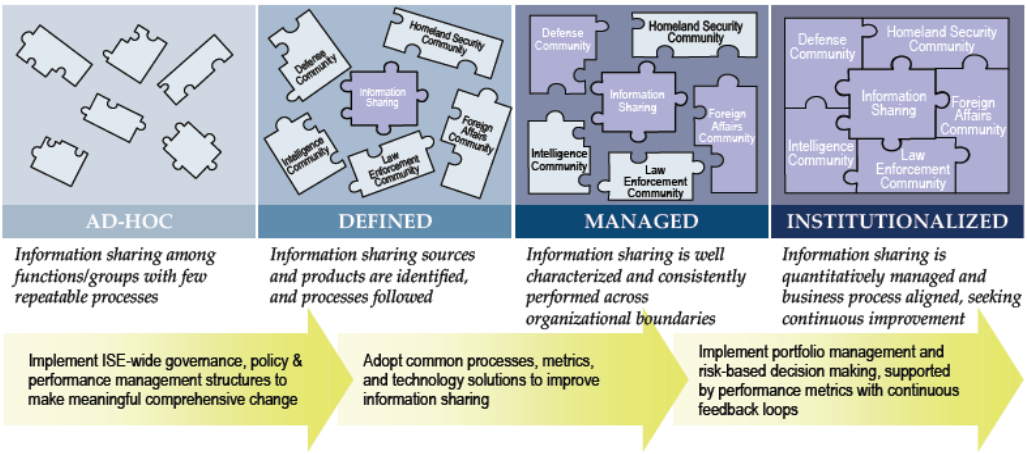

Figure 11. ISE Maturity Model Concept (From Enterprise Architecture Framework Version 2.0, 2008, p.33)

The document asserts, "building on existing systems and capability, the ISE is a system of policies, business practices, architectures, standards, and systems that enable routine, controlled information sharing among all ISE participants" (McNamara, 2009, p. 2). The report also claims that the "ISE has become the most developed information sharing environment in government, the central focal point for terrorism-related information sharing at all government levels, and a model for replication of information sharing elsewhere in the government" (McNamara, 2009, p. 2).

That said, in the months before the 2009 report was released, the following statements were documented by high level practitioners/partners in the terrorism information-sharing community:

From a former U.S. Attorney:

> In my view, the [information sharing] initiatives have cost a lot of money, put lots of people to work, put new technologies into the public service, and given agency officials political cover with the

> illusion of progress, but have not produced meaningful information sharing and have had virtually no operational impact. (McKay, 2008, p. 3)

The CEO of the National Native American Law Enforcement Association stated:

> There may be too many Federal Intelligence and Information Sharing groups within the Federal Government that appear to duplicate or replicate Intelligence dissemination. Many Tribal departments do not have the staff to participate in multiple groups and compare and analyze which one best serves their need for a particular vulnerability or threat." (Edwards, 2009, p. 4)

And similarly, the Director of the Iowa Intelligence Fusion Center commented that "...we don't yet have a single place to go for information...I have, by the way, nearly 30 passwords to change every quarter...what should take 30 seconds takes 30 minutes..." (Porter, 2008, p. 12).

The Government Accounting Office came to a similar conclusion: "Our review showed that the performance measures used to assess the ISE's progress focus on counting activities accomplished rather than results achieved and are not presented in a way that explains how they represent progress toward attaining strategic goals" (GAO, 2008, p. 8). In general, these examples reveal a disconnect between the user community and the policy makers regarding the success of the ISE over the past five years. Perhaps one of the best descriptions of the complexity of the ISE goals is provided by the DoD Information Sharing Implementation Plan:

> The ISE Shared Space enables uniformity in the information exchange of terrorism-related information. It is built in accordance with the ISE Enterprise Architecture Framework and is the IT infrastructure for information sharing. The ISE Shared Space enables each ISE participant to make terrorism-related information, applications, and services accessible to ISE users in each of the three security domains (TS/SCI, Secret/Collateral, and SBU/CUI). More specifically, the Shared Space is where the ISE elements are standardized through the implementation of common terrorism information sharing standards. Physically, the Shared Space is a

> set of hardware and software on a protected/secure network that is exposed at the boundary of an ISE participant's internal network—intranet. Alternatively, it may be hosted by a third party (e.g., another ISE participant), while remaining under the participant's funding, management, and control. (DoD, 2009, p. 31)

H. CONCLUSION

The strategies reviewed in this chapter provide overarching principles for sharing information between federal, state, local and private sector/mission partners. Table 3 recaps the major focus areas for each strategy.

Table 3. Comparing the Strategies: Major Focus Areas / Key Words

Document	**Major Focus Areas / Key Words**
NSIS	Governance: IRTPA/EO's, ISE/ISC, NCTC, ITACG, Fusion Centers, ISACs
DOD ISS	Culture, Policy, Governance, Economic and Resources, Technology/Infrastructure, Mission Partners
DHS ISS	Fusion Center Integration, ISE Coordination, Recognize/Integrate External Organizational Needs Into DHS ISE, Ensure DHS Technology Platforms Facilitate Information Sharing With Partners
USIC ISS	Governance, Policy, Technology, Culture and Economics, Information Discoverability, Retrieval, Accessibility, Trust, Collaboration, "Single Information Environment"
DoJ LEISP	Single Point of Contact for Law Enforcement Sharing, Uniform Policies, Procedures, Foundation for Reaching Partners through the ISE
FBI NISS	Move to a Responsibility to Provide, Create Culture of Sharing, Effective Information Technology Platforms, Work with Information Sharing Entities, ISE focus

There is agreement among the strategies that breaking down cultural barriers, improving sharing practices and collaboration, developing policies and procedures, as well as institutionalizing sharing as a way of doing business are all valid goals. The NSIS specifically states that the ISE is the place for all this to occur across the five communities: intelligence, law enforcement, defense, homeland security and foreign affairs (National Strategy for Information Sharing, 2007, p. 15). Likewise, the various strategies acknowledge the NSIS

requirements, yet at the same time, the respective organizations have maintained a degree of autonomy by keeping their working models (fusion center, ISAC and JIACG) functioning. This may be because the ISE is a strategic "work in progress" that has had mixed results, leaving agencies to continue using existing models that support their missions. This approach would ensure continuity of effort until an effective ISE is functioning as advertised.

As shown Figure 12, all three of the policy model options under examination are in the "current" container. (Each entity predates the information-sharing strategies reviewed.)

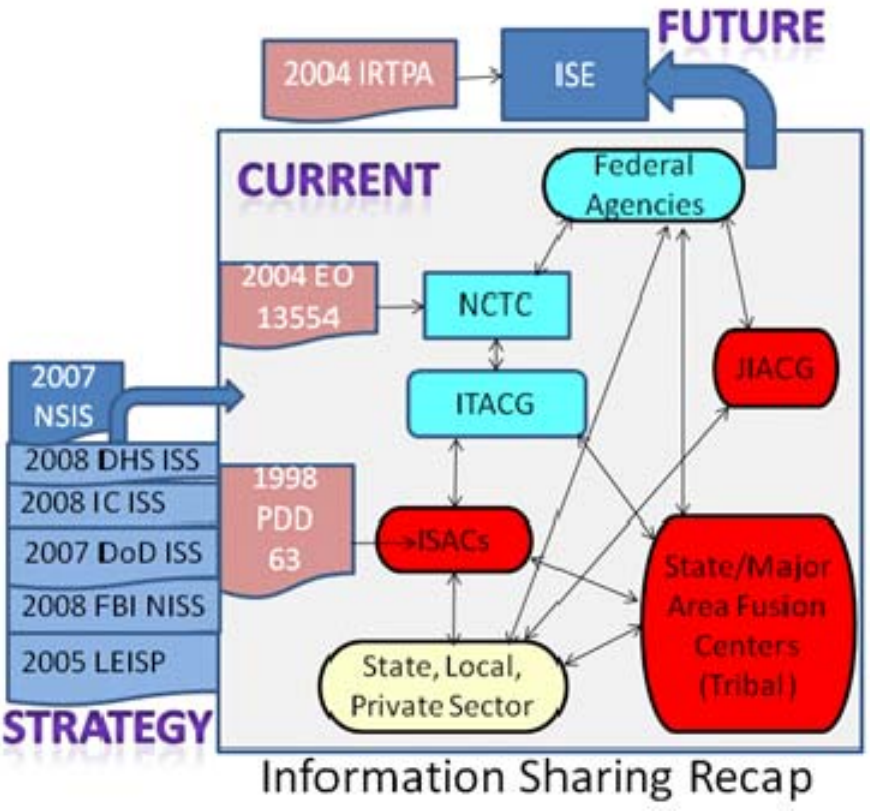

Figure 12. Information Sharing Strategy and Outcome

Likewise, the graphic indicates that there is some level of homeland security/defense information flow overlap since each provides connectivity between federal, state and local communities of interest. The bottom line is that the current way of "doing business" does not point to one optimal solution for

information sharing (intended to be the ISE). With that in mind, a review of each of the three policy model options will attempt to determine which would be best suited to support Arctic policy partners.

IV. STATUS QUO—FUSION CENTER CONSTRUCT

This chapter begins with a brief overview of two core documents: 1) *Fusion Center Guidelines*, which provides background information on fusion centers to include a definition and foundational guidelines, and 2) *Baseline Capabilities for State and Major Urban Area Fusion Centers,* which details subsequent target capabilities. The intent is to provide a context for the model construct under review using the existing federal government strategy for building and maintaining fusion centers. The core documents summary is followed by a review of the existing fusion center in Alaska (status quo model): "Alaska Information Sharing and Analysis Center." The goal is to inform the reader of the viability of this model as an existing information-sharing construct for Arctic region partners.

A. FUSION CENTER GUIDELINES

Published in August 2006, this document provided the following definition for a fusion center: "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity" (DHS & DOJ, 2006, p. 2).

The guidelines document also explains the makeup of a fusion center:

> The primary components of a fusion center are situational awareness and warnings that are supported by law enforcement intelligence, derived from the application of the intelligence process, where requirements for actionable information are generated and information is collected, integrated, evaluated, analyzed, and disseminated. Other key components resident in the fusion center include representatives of public safety, homeland security, the private sector, and critical infrastructure communities. Important intelligence that may forewarn of a future attack may be derived from information collected by local, state, tribal, and federal law enforcement agencies; public safety agencies; and private sector

> entities through crime control and other normal activities, as well as by people living and working in our communities. (DHS & DOJ, 2006, p. 12)

Figure 13 diagrams the components participating in the fusion center construct.

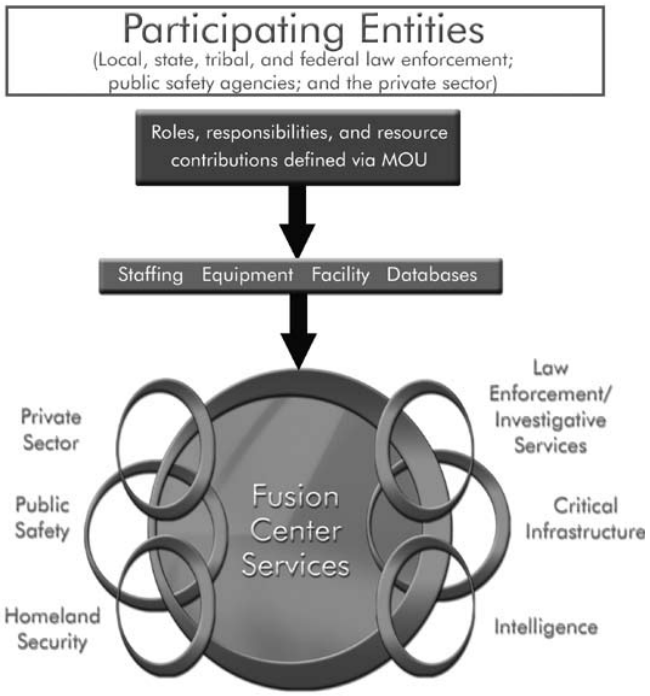

Figure 13. Fusion Center Components (From DHS & DOJ, 2006, p. 13)

The document also states, “These guidelines should be used to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities (DHS & DOJ, 2006, p. 2). The text acknowledges that a wide variety of organizations contribute to a successful fusion center. For example, “public safety and private sector components are integral in the fusion process because they provide fusion centers with crime related information, including risk and threat assessments, and subject matter experts who can feed and threat identification” (DHS & DOJ, 2006, p. 2).

Similarly, the “nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be ‘fused’ with law enforcement data to provide meaningful information and intelligence about threats and criminal activity” (DHS & DOJ, 2006, p. 3). This approach is especially important, given the wide variety of organizations that make up the Arctic region partners. Finally, “ideally, the fusion center involves every level and discipline of government, private sector entities, and the public, though the level of involvement that some of these participants will vary based on the circumstances” (DHS & DOJ, 2006, p. 3). Shown in Figure 14 and as described by the Homeland Security Council, the act of “fusing” is:

> …the overarching process of managing the flow of information and intelligence across levels and sectors of government and the private sector to support the rapid identification of emerging terrorism-related threats and other circumstances requiring intervention by government and private-sector authorities. (DHS, Homeland Security Advisory Council, 2005, p. 3)

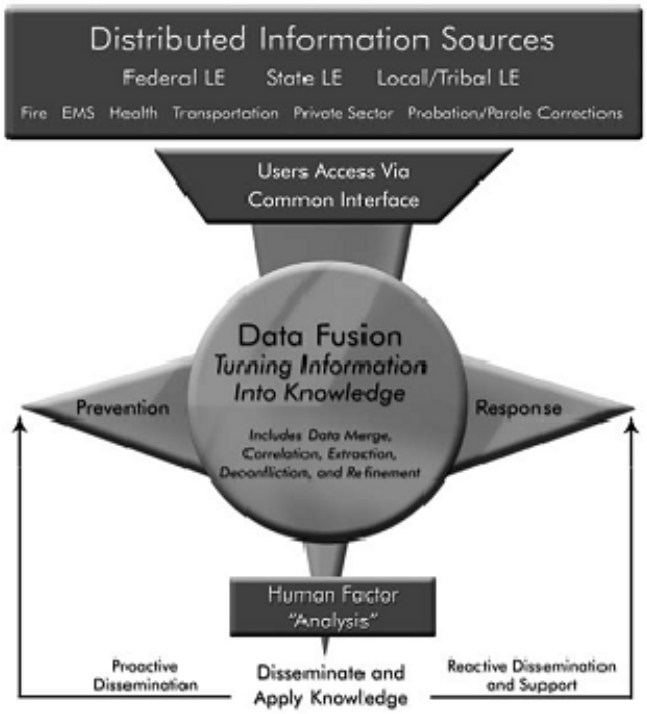

Figure 14. Fusion Process (From DHS & DOJ, 2006, p. 11)

In general then, the intent is for fusion centers to gather, process and disseminate intelligence and information horizontally to stakeholders as well as vertically to the federal level. Before these guidelines were produced, many fusion centers had been operating according to their mission sets. Captured in Table 4 are the set of standards (18 guidelines) for establishing and operating fusion centers. The intent of providing these in their entirety is to inform the reader of how comprehensive they are, keeping in mind that these will also "guide" the Alaska fusion center organizers.

Table 4. Synopsis of Fusion Center Guidelines.

Guide-line	**Description**
1	Adhere to the tenets contained in the *National Criminal Intelligence Sharing Plan* and other sector-specific information-sharing plans, and perform all steps of the intelligence and fusion processes.
2	Collaboratively develop and embrace a mission statement, and identify goals for the fusion center.
3	Create a representative governance structure that includes law enforcement, public safety, and the private sector.
4	Create a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector.
5	Utilize Memoranda of Understanding, Non-Disclosure Agreements, or other types of agency agreements, as appropriate.
6	Leverage the databases, systems, and networks available via participating entities to maximize information sharing.
7	Create an environment in which participants seamlessly communicate by leveraging existing systems and those currently under development, and allow for future connectivity to other local, state, tribal, and federal systems. Use the U.S. Department of Justice's Global Justice Extensible Markup Language Data Model and the National Information Exchange Model standards for future database and network development, and consider utilizing the Justice Information Exchange Model for enterprise development.
8	Develop, publish, and adhere to a privacy and civil liberties policy.
9	Ensure appropriate security measures are in place for facility, data, and personnel.
10	Integrate technology, systems, and people.
11	Achieve a diversified representation of personnel based on the needs and functions of the center.

Guide-line	Description
12	Ensure personnel are properly trained.
13	Provide a multi-tiered awareness and educational program to implement intelligence-led policing and the development and sharing of information.
14	Offer a variety of intelligence services and products to customers.
15	Develop, publish, and adhere to a policies and procedures manual.
16	Define expectations, measure performance, and determine effectiveness.
17	Establish and maintain the center based on funding availability and sustainability.
18	Develop and implement a communications plan among fusion center personnel; all law enforcement, public safety, and private sector agencies and entities involved; and the general public.

1. Baseline Capabilities for State and Major Urban Area Fusion Centers (Capabilities)

The guidelines were supplemented by the Capabilities document in September 2008. This document also refers to the *National Strategy for Information Sharing* goal of establishing a national integrated network of state and major urban area fusion centers and how these capabilities ultimately "assist in ensuring that fusion centers have the basic foundational elements for integrating into the national Information Sharing Environment (DHS & DOJ, 2008, p. 2). (Recall the current functioning status of the ISE from Chapter III.) The document then walks through each of the 18 original guidelines and provides capabilities that, once completed, will place the fusion center in alignment with the guidelines.

On more than one occasion, the document states that the fusion centers may rely on each other to provide specific capabilities, since one of the fusion center guidelines founding principles is to "leverage existing resources and expertise where possible" (DHS & DOJ, 2008, p. 2).This document, as well as the NSIS, respects that a "fusion center's mission should be defined based on local needs" and that there is an option to be "all-crimes" or "all-hazards," stipulating that an "all hazards approach is not a baseline capability" (DHS &

DOJ, 2008, p. 7). These statements point to the overarching intent that there is no “one size fits all;” in other words, there is a high degree of flexibility in developing a fusion center.

The capabilities document is divided into two sections as described below.

a. Section 1

Describes the tasks that need to be completed in order to support the fusion process. To a large degree, these functions mirror the intelligence cycle steps: planning and direction, collection, processing/collation, analysis, dissemination, reevaluation” (DHS & DOJ, 2008, p. 9).These tasks are summarized in the table below:

Table 5. Summarized Fusion Center Process Task Descriptions

Area	**Task Descriptions**
Planning/Direction	Coordinate with other fusion centers; Conduct/contribute to risk assessments; Define information requirements; Develop suspicious activity reporting; Disseminate alert warnings/notifications to State, Local and Tribal authorities, private sector and general public; Situational awareness reporting; Data source definition (what is necessary to conduct analysis); Coordinate with response and recovery officials; Coordinate information sharing with private sector and critical infrastructure and key resources; Participate in exercises
Gathering/Collection	Information gathering reporting strategy; Implement a feedback mechanism; Collect and store information
Processing/Collation	Information collation; Validate/assure reliability and relevancy of information
Analysis/Production	Analytical products (what will be provided and how the product will be disseminated); Training plan; Information linking; Analysis services for the jurisdiction; Open-source analysis capability; Analyst specialization skills and analytical tools.
Dissemination	Dissemination plan; Reporting to other centers and Federal partners.
Reevaluation	Develop and implement a performance evaluation plan.

b. Section 2

Focuses on managing a fusion center, with functional areas that include: management/governance, information privacy protections, security, personnel and training, information technology, and funding as summarized in Table 6 (DHS & DOJ, 2008, p. 9).

Table 6. Summarized Fusion Center Management Task Descriptions

Area	**Task Description**
Management/Governance	Mission statement; Collaborative environment for stakeholders; Policies and procedure manual; Performance measurements; Outreach to leaders and policymakers, public, private, media, and citizens.
Information Privacy/ Protection /	Privacy official; Policy; Protection; Outreach; Accountability
Security	Security Measures; Policy; Procedures; Security Officer, Information security
Personnel/Training	Staffing plan; Background checks; Training Plan
Information Technology, Equipment, Systems Facility, and Physical Structure	Business Processes; Information Exchange; Communications Plan; Contingency and Continuity of Operations Plans
Funding	Investment Strategy to achieve and sustain capabilities

In summary, these documents provide the guidelines and capabilities for the operation of fusion centers, including the Alaska Information Analysis Center.

B. ALASKA FUSION CENTER—ALASKA INFORMATION ANALYSIS CENTER (AKIAC)

Prior to reviewing the current status of the AKIAC ("Center"), it is prudent to understand the genesis and chronology of the organization and how it fits within the larger state homeland security picture.

As stated in the literature review, the mission statement of the state of Alaska, Division of Homeland Security and Emergency Management (DHS&EM) provides that the organization is the "single, statewide focal point for coordinating the State's efforts to prevent terrorist attacks, reduce Alaska's vulnerability to

terrorism, and minimize the loss of life or damage to critical infrastructure, and recover from attacks if they occur" (State of Alaska, 2010).

DHS&EM coordinates the state's homeland security strategy/plan with the State Emergency Response Plan and with the homeland security and disaster plans of the federal government. This is in line with the guidelines document, which states, "the fusion process should be organized and coordinated on a state level, and each state should establish and maintain an analytic center" (DHS & DOJ, 2006, p. 14). In support of the state's mission, one goal of the 2006/2007 Alaska State Homeland Security Strategy (AKSHSS) was to *strengthen information and intelligence sharing* (State of Alaska, 2006, p. 8). One of the steps to accomplish this goal was to "analyze the integration of existing interagency information sharing processes into a statewide fusion center" (State of Alaska, 2006, p. 8).

In October of 2007, the status of the AKIAC was described in a Government Accounting Office report to Congress (based on interviews with the directors of each fusion center), which read:

> The Alaska Fusion Center is in the advanced planning stage with the major concentration being on defining the missions, developing the governance, and outlining potential products and services. The fusion center will be a combined effort of the Alaska Department of Public Safety and the Alaska Division of Homeland Security and Emergency Management. While they do not have a physical fusion center, planning officials have partnerships established with the FBI, other federal and state law enforcement, the U.S. Attorney's Office, the U.S. Coast Guard, the military, and the Federal Emergency Management Agency (FEMA). Through these partnerships, the member agencies already share information and coordinate activities. The officials said that they are considering the advantages of a joint, permanently staffed facility. If feasible and advantageous, they will plan to build or move into an available facility in the future.
>
> The Alaska Fusion Center will have an all-crimes, all-hazards, and all-source scope of operations. As a result of Public Safety and Homeland Security and Emergency Management involvement in developing the fusion center, the center will have both law

> enforcement and emergency management components. All-source includes law enforcement as well as economic information and infrastructure issues. The center will have three focus areas: day-to-day compilation, distillation, and distribution of information products; analyses and assessments of patterns and trends in the risks, threats, and hazards facing Alaska; and serving as an operational planning group serving all agencies when a threat emerges or a disaster occurs. The center has access to DHS's Homeland Security Information Network (HSIN), Department of Justice's Law Enforcement Online (LEO), and the Department of Defense's Secret Internet Protocol Router Network (SIPRNet). (GAO, 2007, p. 53–54)

The 2006/07 strategy and GAO report predate a November 28, 2007 letter from the DHS Secretary Chertoff and the DoJ Attorney General Mukasey sent to the governor of Alaska. The letter describes the ISE, IRTPA, NSIS and the establishment of an integrated network of fusion centers as previously mentioned in Chapter III (Chertoff & Mukasey, 2007). The letter also referenced Guideline 2 above and proffered that DOJ and DHS will work with governors to designate fusion centers and coordinate information sharing using an all crimes approach (Chertoff & Mukasey, 2007). The letter requested that if there is no state organization that it is currently functioning in this capacity, that the state reach out to the National Fusion Center Coordination Group for support using the contact information provided (Chertoff & Mukasey, 2007). Apparently, DHS/DOJ were unaware of the GAO report and status of the developing center as noted above.

The following year, the 2008 AKSHSS contained the identical verbiage for strengthen information and intelligence sharing: "analyze the integration of existing interagency information sharing processes into a statewide fusion center" (State of Alaska, 2008, p. 11). The 2009 strategy added the word "virtual" in front of "statewide fusion center," otherwise the text was unchanged from the previous two iterations" (State of Alaska, 2009, p. 15).

The strategies themselves do not indicate that progress has been made to date regarding the development of a "fusion center." However, in September of

2009, the new Alaska governor responded to the 2007 letter from the Attorney General and Secretary of DHS. The letter acknowledges the recent establishment of the AKIAC, located in the FBI field office in Anchorage, Alaska. The governor's letter also stated that the AKIAC is "responsible for coordinating the gathering, processing, analysis, and dissemination of terrorism and law enforcement information in Alaska and will serve as the state's designated primary 'fusion center' in the Information Sharing Environment" (Parnell, 2009).

That same year, the governor described the functionality of AKIAC in a press release:

> The Department of Military and Veterans Affairs [DHS&EM is nested within this organization] collaborated with the Department of Public Safety to establish a Fusion Center and Alaska Information Analysis Center for information sharing and analysis and to become part of the national Information Sharing Environment. This resulted in faster and more efficient response to threats to Alaska and infrastructure (Parnell, 2009).

Also in 2009, the National Fusion Center Coordination Group labeled the *Alaska Statewide Law Enforcement Information Center* in Anchorage as one of 50 "Primary Designated Fusion Centers." This means that the center is:

- Designated by the Governor as the primary state center
- Responsible for passing relevant homeland security information received from the federal government to other centers in the state as well as to nonparticipating law enforcement agencies
- Agrees to follow the Fusion Center Guidelines and work toward attaining the Baseline Capabilities for fusion centers
- Managed and run by the state, or the state's designee, in which the center is located
- Receives some level of federal support (grant monies, deployment of federal personnel, IT systems, and/or security clearances)
- Comprises two or more state or local agencies. (National Fusion Center Coordination Group, 2009)

As of 2010, the Concept of Operations (CONOPS) and policy manual for the AKIAC are still in draft form. However, these draft documents do provide insight into the existing capabilities and direction the center is headed. The current vision and mission statements are:

> Vision: "to provide a centralized, comprehensive, multiagency, information sharing network to enhance their strategic and operational effectiveness of all Alaska public safety agencies involved and crime prevention, crime investigation, counterterrorism and homeland security." (Alaska Information Analysis Center [AKIAC], 2009a, p. 1)
>
> Mission: "to evaluate, analyze, and disseminate information regarding criminal, terrorist and homeland security activity in the state of Alaska while complying with state and federal law to ensure the rights of privacy at all. (AKIAC, 2009a, p. 1)

The CONOPS provides that "the AKIAC is established to provide a central clearinghouse for information sharing focusing on homeland security, organize criminal activity and all hazards within and surrounding the state of Alaska" (AKIAC, 2009a, p. 1). The organization will accomplish this mission by producing and disseminating: bulletins and assessments; investigation and analysis support of suspicious activity reports; responding to requests for information and requests for service for members and customers; collaboration with federal state and local agencies to produce joint products; coordinating/facilitating regional training opportunities; identifying patterns and trends; and assisting in the coordination and the deconfliction of information between members and customers.

The goals and objectives of the center are to facilitate information sharing among all levels of government and the private sector. These include defining collection requirements, providing a central dissemination point, supporting significant incident responses, and establishing the organization as the primary contact for law enforcement and homeland security information sharing in the state (AKIAC, 2009a, p. 2).The intent is to increase the decision-making capabilities of state and local leadership by collecting, managing, and distributing

strategic and tactical information and developing and implementing useful and meaningful products, processes and tools for information analysis. Additionally, the organization will develop a plan to sustain operations, an outreach/liaison program, and operating policies to include privacy, funding, training and evaluation.

Governance for the AKIAC is an executive committee that includes the three major stakeholders: AST, AK DHS&EM, and FBI. These members determine the policies and procedures, with overall guidance and support of the organization being the responsibility of Alaska Department of Public Safety (DPS), which oversees the AST. The AKIAC is currently staffed with a representative from each participating agency at their own expense. The members work with DHS and other state and federal agencies to create statewide threat assessments, which are then used to create collection requirements based on the risks identified. Bi-directional information flows from regional law enforcement investigative groups, statewide task forces, participating agency representatives, liaison officers and other fusion centers. The organization reviews this information to identify threats and trends, and produces information bulletins that are then disseminated to registered members.

The center also provides training regarding collection requirements to customers of the center, which include law enforcement, first responders, government and private-sector personnel (AKIAC, 2009a, p. 3). The organization is pursuing development of “a statewide information liaison officer program designed to expand membership and information” (AKIAC, 2009a, p. 6). While the current funding situation relies on each participating agency to provide support to the organization out of existing budgets, the center expects to identify additional sustainable funding options via the grant application process (AKIAC, 2009a, p. 6).

As mentioned earlier, the policy manual for the center is also currently under development. The draft document identifies the functions and responsibilities for participants assigned to or working within the organization.

The policy states that the center's viewpoint is statewide, with a particular focus on critical infrastructure, weapons of mass destruction and homeland security (AKIAC, 2009b, p. 1).The staff is expected to respond to any valid requirements for products or services based on approved priorities and manpower (AKIAC, 2009b, p. 3). The Center operates during the weekday from 8:00 a.m. to 4:30 p.m. During these hours, members receive, as well as disseminate, various electronic documents, presentations and other intelligence related products via a DPS networked computer server. The manual discusses the option to have members link into their organizational networks in addition to utilizing the DPS local area network. This allows for multiple options to share information as well as connect to various Web-based databases.

The procedures for handling information are situationally dependent. Members receive information through various queries to include other law enforcement organizations and directly from the public. Responses may be made in person or by telephone, electronic mail, fax, letter or a detailed intelligence product, and all within compliance of applicable regulations (AKIAC, 2009b, p. 3). Information that leads to intelligence is stored in the statewide law enforcement intelligence database. The policy acknowledges the value of collected information and ensures dissemination to personnel, teams or agencies for "analysis, training and other purposes (AKIAC, 2009b, p.4).

In order to fully balance the assessment of whether or not this model could support Arctic policy partners (given that this is the status quo/nationally recognized construct for homeland security information sharing), the researcher investigated the center's past funding shortfalls. A cursory review of the fusion center grant awards (investment justification submitted by the state of Alaska) over the past several years provided additional insight into this limitation.

For example, in 2006, $557,000 in Homeland Security Grant Funding was allocated to the Alaska Information Coordination Center (AICC) then aka "fusion center (Federal Emergency Management Agency [FEMA], 2008, p. 57). The 2007 investment justification shows that AICC was part of a $1.5 million funding

distribution (FEMA, 2009, p. 5). The 2008 investment justification (#8) is labeled "Strengthen Information Sharing and Collaboration Capabilities" with a corresponding statement that "Alaska does not operate a 'brick-and-mortar' fusion center, and this investment will support our continued efforts to collaborate and share information and intelligence in a virtual setting where possible (FEMA, 2009, p. 58).

The baseline description in this document also claims:

> The State Emergency Coordination Center [part of DHS&M] continues to produce, refine, and disseminate intelligence and information on all-hazards events. Daily, weekly, and event-driven situation reporting is in place. The Anti-Terrorism Advisory Council of Alaska (ATACA) and their Joint Coordination Group and Intelligence Advisory Group continue to provide coordinated law enforcement and counter-terrorism related information and intelligence. The member organizations of the ATACA continue to work directly with the Joint Terrorism Task Force, the Department of Defense, and the State of Alaska. Critical Infrastructure/Key Resource owners, operators, and government agencies continue to share information and intelligence through organizations like the Alaska Partnership for Infrastructure Protection and InfraGard. (FEMA, 2009, p. 57)

The link between the above organizations/partnerships and the AKIAC is unclear. (Recall that in 2009 the governor stated that the AKIAC is "responsible for coordinating the gathering, processing, analysis, and dissemination of terrorism and law enforcement information in Alaska... serve[ing] as the state's designated primary 'fusion center' in the Information Sharing Environment (Parnell, 2009).

Finally, the 2009 state investment strategy only mentions "fusion center" with regard to the 2006 grant funding (FEMA, 2009, p. 5). Investment #1 is "Strengthen Planning and Preparedness (FEMA, 2009, p. 5). The purpose statement provides that:

> This Investment integrates four previous investments, reflecting inherent linkages and shared strategies among planning and preparedness, regional collaboration, and information sharing.

> Regional and statewide planning workshops, training, and exercises foster regional collaboration, information sharing, and the ability to respond and communicate effectively with partners within and across communities...Information and intelligence sharing will further develop as partner agencies continue statewide planning. (FEMA, 2009, p. 5)

The step towards "integration of existing interagency information sharing processes into a virtual statewide fusion center" as part of Goal 4, *Strengthen Information and Intelligence Sharing,* in the 2009 AKSHSS is not referenced as part of the investment justification (State of Alaska, 2009, p. 15). Whether "brick and mortar" or "virtual," the most recent funding investments appear to exclude the AKIAC (documented fusion center) in favor of a variety of previously established information-sharing organizations.

This spending approach seems counter to the intent of previous grant funding, and disagrees with the fiscal year 2010 DHS grant guidance. In this document, DHS highlights the purpose of the State Homeland Security Program (SHSP) to provide "funds to build capabilities at the state and local levels and to implement the goals and objectives included in *state homeland security strategies* [emphasis added] and initiatives in their State Preparedness Report" (DHS, 2010, p. 3).

Likewise, DHS prescribes that funding is specific for fusion centers:

> ...consistent with the *Implementing Recommendations of the 9/11 Act of 2007* (Public Law 110-53) (9/11 Act), states are required to ensure that at least 25 percent of SHSP appropriated funds are dedicated towards law enforcement terrorism prevention-oriented planning, organization, training, exercise and equipment activities, including those activities which *support the development and operation of fusion centers* [emphasis added]. (DHS, 2010, p. 3)

As stated in the *Introduction*, the policy options analysis methodology used for this thesis is the comparison of each model against the criterion as listed

in the matrix below. Table 7 provides a numbered score: low (1), medium (2) and high (3), to indicate the level to which AKIAC complies with the prescribed criterion.

Table 7. AKIAC Capability Analysis

AKIAC (Fusion Center Model) Score 19/27 **Level of capability to meet the prescribed criterion.**		
Low/Minimal **Score = 1**	**Medium/Moderate** **Score = 2**	**High** **Score = 3**
1	**2**	**3**
Criterion 1.0 **Robustness: Resources, Policies, Political Acceptability**	**Criterion 2.0** **Collaboration: Partners, Variety, Frequency**	**Criterion 3.0** **Information Sharing: Systems, Processes, Procedures**
Factors:	*Factors:*	*Factors:*
1.1 Available resources (Personnel, funding, i.e., ability to sustain effort)	2.1 Number of partners (few, some, many)	3.1 Systems used, (Portals/Networks)
Score = 1 No dedicated funding; participating organizations support with existing budgets; small staff	Score = 2 Some partners (mainly law enforcement)	Score = 3 Access to multiple collaborative systems; sharing information at multiple levels
1.2 Policies/Guidance (CONOPS, policy manuals, business rules, etc.)	2.2 Level of collaboration (federal/state/local)	3.2 Processes for information sharing/dissemination (templates, forms, contact lists, databases, etc.)
Score = 2 In draft form; being worked	Score = 3 Collaborating at all levels	Score = 2 Some working processes still being defined; (drafts)
1.3 Political Acceptability (Level of support or opposition)	2.3 Frequency of collaboration (daily, weekly, monthly)	3.3 Standard Operating Procedures (e.g. instructions for collecting and disseminating information)
Score = 1 Focused primarily on law enforcement	Score = 3 Daily collaboration	Score = 2 Some working procedures still being defined; (drafts)

The analysis indicates a score of 19/27, reflecting that the AKIAC has an overall moderate level of capability to meet the prescribed criterion. This model's score was lowered by the lack of robust funding/resources, corresponding policies, processes and procedures that remain in draft form, limited partners and

political acceptability based on current law enforcement focus. The organization has created a mission statement, is working on policy, procedures and training, sharing intelligence and information, leveraging available databases, systems, and networks, offering services and products to customers and determining the effectiveness of these efforts. In summary, the center appears to be following the fusion center guidelines and capabilities to the extent possible given the limited staff. Without the capability to “establish and maintain the center based on funding availability and sustainability,” it may be difficult for the organization to act as a viable model that could support Arctic region partners (DHS & DOJ, 2006, p. 63).

THIS PAGE INTENTIONALLY LEFT BLANK

V. JOINT INTERAGENCY COORDINATION GROUP (JIACG) MODEL

As mentioned in Chapter I, the U.S. Northern Command (USNORTHCOM) JIACG model was selected for review for two main reasons: 1) the command shares the homeland defense mission within the Arctic region (as shown in Figure 15), and 2) the organization's established information-sharing relationships with many of the other relevant equity partners at the national level.

Figure 15. USNORTHCOM's Arctic Area of Responsibility (From DoD, 2010)

Before reviewing USNORTHCOM's structure, a short background on the history of the JIACG concept is in order. According to the DoD *Dictionary of Military and Associated Terms*, a JIACG is:

> An interagency staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners. Composed of US Government civilian and

> military experts accredited to the combatant commander and tailored to meet the requirements of a supported joint force commander, the joint interagency coordination group provides the joint force commander with the capability to coordinate with other US Government civilian agencies and departments. (DoD, 2009, p. 290)

The JIACG concept was conceived after experimentation by U.S. Joint Forces Command (JFCOM), Joint Warfighting Center, Joint Innovation and Experimentation Directorate in early 2001. The groups were designed to improve planning and coordination between DoD staffs and civilian agencies of the U.S. government (USG), which initially were focused mainly on the international "war on terrorism" and humanitarian support overseas (U.S. Joint Forces Command [JFCOM], 2007, p. vi). JFCOM claims that the "JIACG provides the critical linkage between the military and engaged U.S. government agencies that allow the coordinated application of all instruments of national power (JFCOM, 2007, p. II-1). JFCOM's intent was to test the idea of "placing a civilian oriented interagency element on combatant commander staffs (JFCOM, 2010). The group was expected to coordinate at the headquarters staff level daily, providing continuous advice/interagency subject matter expertise on civilian agency operations, capabilities and limitations. Among other functions, the JIACG would also provide the perspective of civilian agencies to all military operational planning activities and exercises. This would allow the military to better understand how civilian agencies approach a situation in which they would likely end up working together.

In October 2001, the Secretary of Defense directed that all combatant commanders were authorized to develop JIACGs and "liaise directly with the appropriate agencies to explore needed capabilities and relationships to support theater counterterrorist operations" (Bogdanos, 2007, p. 4). This guidance allowed for flexibility among the combatant commanders in how they employed their JIACGs. Implementation was based on the mission focus of each combatant command, so naturally the first JIACG's had different structures and

members. For example, U.S. Pacific Command's JIACG focused almost exclusively outwardly on counterterrorism in their area of responsibility (Marks, 2005, p. 8).

By the time USNORTHCOM stood up in October 2002, the JIACG was an accepted governmental entity. With USNORTHCOM's new mission, "anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests," the organization had a natural reason to embrace the JIACG concept (USNORTHCOM, 2010). Figure 16 highlights the civil support missions that would require interagency coordination.

Figure 16. NORAD/USNORTHCOM Missions (From Catalino, 2009, p. 5)

Indeed, the command developed an entirely separate directorate for Interagency Coordination (IC), under which its JIACG falls. According to a recent *Interagency Coordination* briefing, the USNORTHCOM IC provides an operational level interagency context for the commander (USNORTHCOM Interagency Coordination [USNC IC] Division Chiefs, 2010, p. 3). Their mission is to "facilitate the integration and synchronization of interagency activities to ensure mutual understanding, unity of effort (Catalino, 2009, p. 3). The IC is

divided into four divisions: operations, planning and synchronization and capabilities and outreach. Under these divisions are: training and exercise, preparedness and planning, law enforcement/ security, concepts and technology and private sector integration as shown in Figure 17.

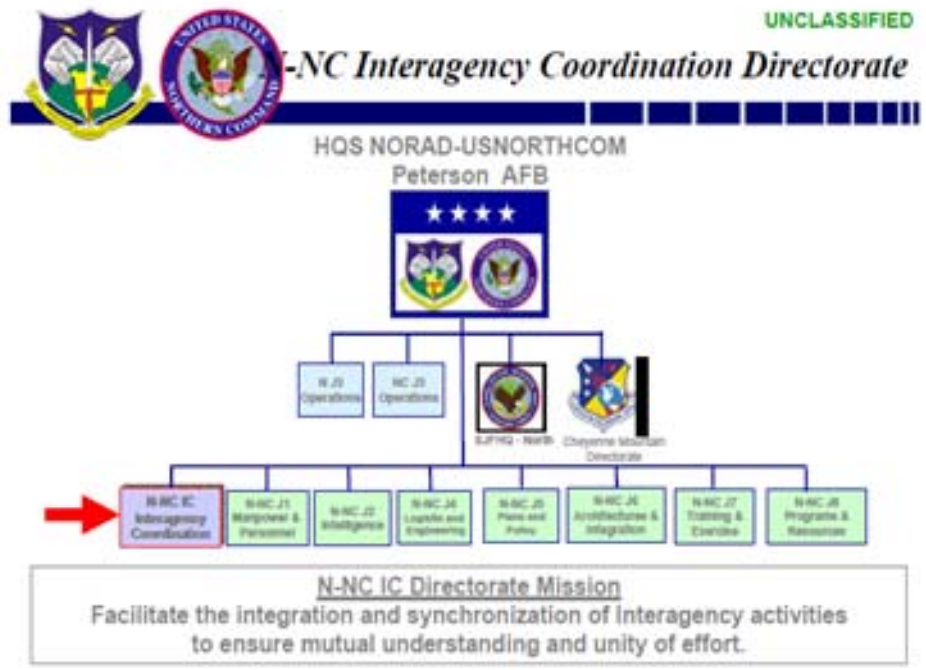

Figure 17. NORAD/USNORTHCOM Missions (From Catalino, 2009, p. 10)

While early JIACGs may have generally fallen in line with one of three communities: intelligence, political-military or law enforcement, USNORTHCOM's focus is on "mission partners," which includes all three disciplines as well as the private sector (Bogdanos, 2007, p. 6). To exchange knowledge and information, the IC hosts conferences and seminars, as well as bi-monthly JIACG forums with agency participants and other staff. According to the draft *JIACG Strategy*, USNORTHCOM interprets the term "JIACG" to mean the "collective 'body' of the staff and non-DoD agency representatives..." (USNC IC, 2009, p. 6). Many of these agency representatives are resident at USNORTHCOM; others exist in different directorates or are within the local area and provide support when needed.

This type of coordination and synchronization between organizations is intended to provide the Command the ability to reach out to 60+ agencies at all times (19 are resident on a daily basis; the rest can be tapped during surge operations) (USNC IC, 2009, p. x). In 2005, then USNORTHCOM Commander Admiral (ADM) Keating testified that his JIACG "includes 59 resident DoD and non-DoD agency representatives, all of whom provide subject matter expertise to ensure mutual support of homeland defense and civil support missions." As of August 2009, USNORTHCOM's JIACG continued to coordinate with over 60 mission partners, some of which are shown in Figure 18 (Catalino, 2009, p. 5).

Figure 18. USNORTHCOM's Mission Partners (McConnell, n.d., p. 4)

This multi-layered approach is expected to support the development of habitual relationships. Similarly, the JIACG has endeavored to focus outside the "DOD centric mindset to consider the interagency perspective," believing that "it is imperative that USNORTHCOM coordinate, collaborate, integrate, and synchronize with agency partners either in response or in planning" (USNC IC, 2009, p. 5). Therefore, on a day-to-day basis, the JIACG plans to support routine

operational planning and initiatives and manage the flow of information and knowledge regarding civilian organizations relative to military operational planning (USNC IC, 2009, p. 6). This “all of government/whole of society” approach is being used to facilitate the support of homeland defense and civil support operations such as the recent earthquake in Haiti as well as the most recent oil spill response effort in support of the recent sunken offshore drilling rig *Deepwater Horizon*.

In a proactive sense, the JIACG has worked with state organizations to facilitate assessments regarding vulnerabilities such as typhoons, hurricanes, earthquakes, tsunamis and volcanoes (USNC IC, 2009, p. 18). This data allows the group to conduct gap analyses to get an idea of state vulnerabilities and any likely response efforts that might be needed. For that purpose, the group maintains lists of Web sites and state emergency response/mitigation plans, because the organization believes that, “understanding plans capabilities and limitations of other stakeholders is key to building your own plan” (USNC IC, 2009, p. 5).

The JIACG has also provided information on DoD’s domestic security initiatives to non-DoD organizations. For example, USNORTHCOM supports law enforcement requests for assistance along the southwest border when a homeland defense threat is present. It is intended for these types of initiatives to be leveraged by other organizations, which may save on resources while providing unity of effort. In a similar vein, the JIACG can reach-back to other organizations inside the command; initiatives and experience along these lines may be of interest and potential support to Arctic region partners as well (USNC IC, 2009, p. 21).

Likewise, the JIACG is interested in critical infrastructure protection, such as energy grid security, because mission assurance (for defense critical infrastructure) depends on commercial energy, much of which is owned by the

private sector. USNORTHCOM's IC and JIACG have been working to better understand the private sector emergency response capabilities and how the USG fits within those response efforts.

Additionally, the group has reached out to other "for profit" partners such as Wal-Mart's Business Emergency Operations Center, Walgreens Operations Center, Retail Industry Leaders Association, the Red Cross, National Volunteer Organizations National Governors Association, National Emergency Management Association, American Association of Railroad and others during operations (USNC IC, 2009, p. 9). This pre-event interaction and "inclusiveness" is important because during a contingency (especially considering the complicating factors in the Arctic) is not the time for first contact. These efforts are expected to help facilitate coordination of functional activities with agency partners in anticipation of requests for assistance in accordance with the National Response Framework (USNC IC JIACG Strategy, 2009, p. 4).

The IC also works to integrate the private sector into exercises and sharing of best practices. In fact, the organization has drafted a *Private Sector Engagement Marketing Plan* that seeks to increase private sector participation in JIACG meetings, exercises and contingency operations, and develop strategic alliances nationally, internationally, and locally (Catalino, 2009, p. 3). Similarly, the objectives of the draft *Private Sector Integration Implementation Plan* are: enhanced collaboration with private sector partners; better understanding of the private sector requirements, capabilities and missions; enhanced understanding of USNORTHCOM's capabilities and improved national level response to natural disasters and/or incidents of national significance (Catalino, 2009, p. 3).

During an event, the IC intends to stand up an "Interagency Coordination Center" that works within the Homeland Security Information Network to push and pull information between partners. Members of the JIACG work to analyze interagency products like DHS's National Operations Center Daily Reports, Infrastructure Protection Reports and FEMA Daily Operations Briefing and Private Sector Daily Reports. They also review USGS/Department of Interior—

Office of Emergency Management Daily Situation Reports (SITREPs), as well as SITREPs from other organizations such as Department of Transportation, Department of Energy, Environmental Protection Agency, the Transportation Security Operations Center (Freedom Center), U.S. Coast Guard, non-governmental organizations, the private sector and State Emergency Operations Centers (USNC IC, 2009, p.12).

Similarly, the JIACG makes assessments for current operations, future operations and any issues that may be involved based on information from across these other agencies. The assessment shown in Figure 19 provides an understanding of the "big picture" of what is happening during an event.

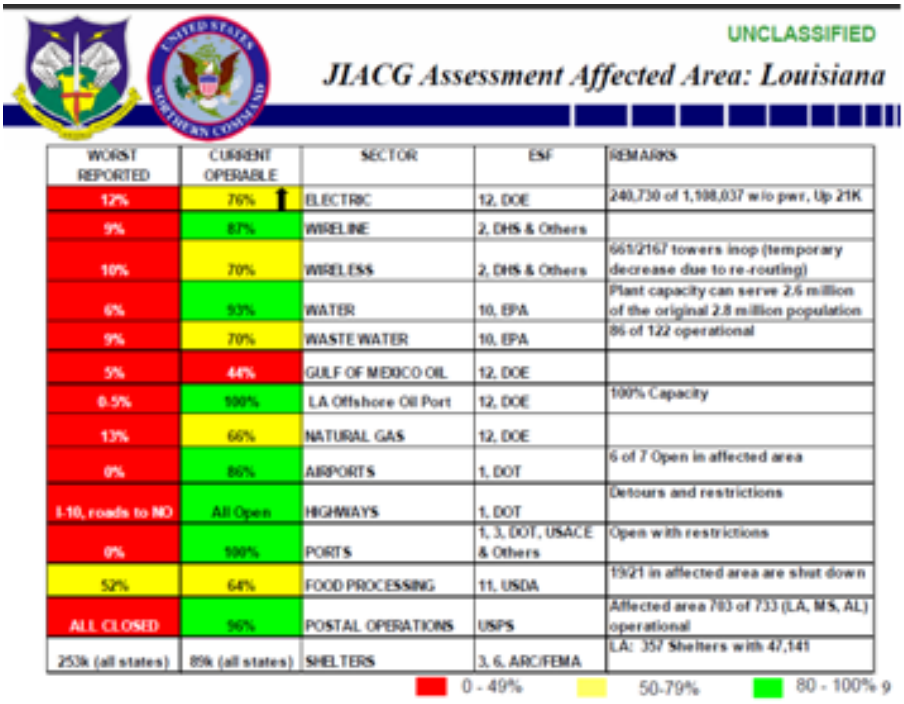

Figure 19. JIACG Assessment Example (USNC IC, 2009, p. x)

Another product that emerges from these analyses is the JIACG *Assessment of Agency Deployments,* which prioritizes the interagency assets/capabilities relevant to potential requests for assistance for DoD (similar/unique) capabilities (USNC IC, 2009, p. 18). Likewise, agencies can

request additional information from USNORTHCOM and push it back to their own organizations. How many are actually doing so has not been quantified.

Admittedly, the information described thus far was provided by the USNORTHCOM JIACG staff. As noted in the Introduction, the intent of this researcher was to balance the model reviews with independent study of related scholarly documents. In this case, the recently released Government Accounting Office report on interagency coordination with regard to homeland defense and civil support missions highlighted where performance could be enhanced within DoD. These areas include: clearly defined roles and responsibilities, performance assessments of liaison personnel, reliance on personal relationships subject to rotation and an institutionalized approach to interagency coordination (GAO, 2010, pp. 27, 33). The GAO document specifically mentions USNORTHCOM, finding:

> ...NORTHCOM officials told us that they lack guidance on determining the appropriate number and selection of agencies from which they should be exchanging liaisons. Officials from ASD/HD acknowledged that DOD currently has a gap in its guidance for determining the appropriate number and selection of agencies and that it plans to issue such guidance in 2010. A DOD-wide staffing-needs assessment would better position DOD to ensure the most appropriate and efficient exchange of liaisons between DOD entities and DOD's federal partner agencies, and thus maximize the effectiveness of interagency coordination efforts. (GAO, 2010, p. 27)

Similarly, the document states that:

> Until position descriptions for liaisons are consistently established, roles and responsibilities for interagency coordination will continue to lack clear definition, and DOD will be unable to assess liaisons from a performance perspective. (GAO, 2010, p. 33)

Based on the GAO's report, it could be argued that although there is a lot of activity, the effectiveness of such activity and partnerships has yet to be measured. Similarly, the draft JIACG strategy/policies, after many years of operation, indicate that there still may not be clear organizational goals/objectives

available for measurement. Additionally, the group's main focus is to provide informational planning for the Combatant Commander. This spotlight points towards a "one-way" pull of information from various systems to the leadership at USNORTHCOM. Even though the intent is to provide information back to the community, the amount/type of information in the form of relevant products, reports, etc. has not been determined, as evidenced by the GAO report. Gathering information, analyzing and providing relevant products back to the community would be of value to the Arctic region partners.

At present, the USNORTHCOM JIACG is a functioning community that interacts with all levels of government and the private sector using developed processes and procedures. Taking the information as provided and completing the criterion matrix as shown in Table 8, USNORTHCOM's JIACG appears to have attained a moderate-high degree of robustness, collaboration and information-sharing capabilities. However, in addition to a lack of prescribed measure of effectiveness for the personnel and products developed, on the surface, it appears that the group is primarily geared towards a "one way pull" of information, which may leave Arctic region partners wanting.

Table 8. JIACG Capability Analysis

JIACG—Score 22/27 **Level of capability to meet the prescribed criterion**		
Low/Minimal **Score = 1**	**Medium/Moderate** **Score = 2**	**High** **Score = 3**
1	**2**	**3**
Criterion 1.0 **Robustness:** **Resources, Policies, Political Acceptability**	**Criterion 2.0** **Collaboration:** **Partners, Variety, Frequency**	**Criterion 3.0** **Information Sharing:** **Systems, Processes, Procedures**
Factors:	*Factors:*	*Factors:*
1.1 Available resources (Personnel, funding, i.e., ability to sustain effort)	2.1 Number of partners (few, some, many)	3.1 Systems used (Portals/Networks)
Score = 2 Dedicated funding for staff; participating organizations voluntarily support with own	Score = 3 Many partners/stakeholders	Score = 3 Access to multiple collaborative systems; sharing information at

JIACG—Score 22/27 **Level of capability to meet the prescribed criterion**		
Low/Minimal **Score = 1**	**Medium/Moderate** **Score = 2**	**High** **Score = 3**
staff		multiple levels
1.2 Policies/Guidance (CONOPS, policy manuals, business rules, etc.)	2.2 Variety of collaborators (Federal/State/Local/Private Sector)	3.2 Processes for information sharing/dissemination (templates, forms, contact lists, databases, etc.)
Score = 2 Strategy in draft form	Score = 3 Partnering at all levels of government/private sector	Score = 2 Some working plans (Private Sector Engagement /Implementation being defined; (drafts)
1.3 Level of political acceptability (Level of support or opposition)	2.3 Frequency of collaboration (daily, weekly, monthly)	3.3 Standard Operating Procedures (e.g. instructions for collecting and disseminating information)
Score = 1 Focus on Military; mainly information “pull”	Score = 3 Daily collaboration	Score = 3 Procedures in place for collecting data/making assessments

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ALASKA PARTNERSHIP FOR INFRASTRUCTURE PROTECTION (INFORMATION SHARING AND ANALYSIS CENTER CONSTRUCT)

This chapter provides background information on the genesis of Information Sharing and Analysis Centers (ISACs), which sets the stage for reviewing the Alaska Partnership for Infrastructure Protection (APIP) as the third and final model construct under review.

The basis for ISAC models was the 1998 Presidential Decision Directive/National Security Council-63 (PDD-63) *Critical Infrastructure Protection.* This document "strongly encourage[s] the creation of a private sector information sharing and analysis center. The actual design and functions of the center...will be determined by the private sector, in consultation with and with assistance from the Federal Government" (White House, 1998). In many ways, ISACs provide a "fusing" function for critical infrastructure information. The general intent of PDD-63 was for these ISACs to:

> …serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information... about vulnerabilities, threats, intrusions and anomalies...become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used be [sic] the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability. (White House, 1998)

As stated in Chapter III, the *National Strategy for Information Sharing* acknowledged that 85 percent of the infrastructure and resources critical to the nation is in the hands of the private sector (White House, 2007, p. 4). Information sharing efforts in this area have been promoted by the multiple ISAC organizations that have expanded across various infrastructure sectors. Similar to the fusion center approach with the states, the federal government left the

design and operation of ISACs up to the private sector, offering support and coordination via public organizations that facilitated their interests.

According to one of the founding members of APIP, the organization began in the absence of a standing ISAC post 9-11.[9] The state of Alaska (SoA), Department of Defense (DoD) and a few private sector organizations met ad hoc to discuss the protection of critical infrastructure within the region. There was a need for integrated planning between the agencies, yet little forward movement was observed during these meetings. The private sector was concerned with competition and proprietary rules; DoD wanted to classify the information. Resistance to change and an unwillingness to consider alternate solutions were the main reasons the effort stalled.

A select group decided that the private sector's stake needed to be the focal point, since all Alaska critical infrastructure is either owned by or depends on the private sector for support. The private sector had to be convinced of the benefits of a shared, collaborative development process. The group considered a partnership as a means to combine the missions of government and the private sector into a collaborative alliance that could work toward a common homeland security objective. They emphasized breaking down the competitive forces that prevented information sharing and building a partnership that focused on preparing for anti-terrorism activities as a whole (Jensen, 2007, p. 3).

For the purposes of this thesis, the term *partnership* is defined as*:*

> …a cooperative venture between the public and private sectors, built on the expertise of each partner that best meets clearly defined public needs through the appropriate allocation of resources, risks and rewards. (Klitgaard & Treverton, 2003, p. 9)

Likewise, *collaboration* means:

> …any joint activity by two or more organizations intended to increase public value by working together rather than separately. It is an interactive process involving an autonomous group of actors

[9] Personal discussion; historical documentation of this nature is not available.

> who use shared rules, norms, or organizational structures to: solve problems, reach agreement, and undertake joint actions, share resources such as information, money, or staff. (Imperial, 2004, p. 13)

APIP was officially formed in November 2004 with an initial sponsorship of DoD, the SoA and several energy organizations that recognized the need to truly collaborate. It evolved from the critical infrastructure committee of the combined Federal/State Anti-Terrorism Advisory Council established after September 11 and broadened the scope to "all-hazards" in order to leverage efforts. APIP's mission is to "provide an integrated all hazards approach to disruptions, natural or man-made to critical infrastructure throughout the State of Alaska." (APIP Handbook, 2009, p. 1). Basically, APIP is a community that coordinates information sharing among all participants in order to enhance group knowledge related to infrastructure interdependencies, during both routine and contingency events. This "big picture" (versus individual information collection efforts) enables decision making by providing situational awareness for all partners simultaneously.

Initially, the two public organizations took on leadership roles with APIP membership recognizing that the SoA and DoD were better suited to provide the necessary personnel resources required to develop the organization. Likewise, both government organizations recognized that they would be on the receiving end of information; providing personnel and financial resources to research and develop courses of action was the government's way of sharing the responsibility for infrastructure protection. Taking the lead in this way avoided one possible reason for failure, "a low general level of leadership talent or the lack of a 'good government' ethos" (Bardach, 2009, p. 106).

APIP was up against the same political, administrative and technical challenges that confront many organizations attempting to collaborate effectively.

All members were ultimately responsible for overcoming these conflicts, which as noted in *A Manager's Guide to Resolving Conflicts in Collaborative Networks,* include:

> …identifying their own and their organization's interests and needs in advance, as well as researching and thinking about the other parties' interests and needs…focusing on creative solutions that address the procedural, substantive, and relationship (or psychological) needs of all the parties involved. (O'Leary & Bingham, 2007, p. 35)

To meet these various expectations, partners (team members) had to find solutions, be open minded and willing to brainstorm options collaboratively. (Similar expectations will drive the Arctic region partners.) Initially, much of the information flow between APIP partners was ad hoc, informal and based on personal relationships, as shown in Figure 20 (Martin, 2007, p. 5). The challenge for APIP leadership was to persuade members to willingly share propriety data in order to build trust between competitors and regulators. The members also had to trust their government leaders in order to avoid a pitfall noted by the Government Accountability Office, "a lack of trust in DHS and fear that sensitive information would be released are recurring barriers to the private sector's sharing information with the federal government…" (GAO, 2006, cover).

APIP confronted disparate agency authorities, capabilities and information security by working through their partnership to develop memorandums of agreement before integrating processes and procedures. The organization developed a charter (co-chaired by leadership of SoA/DoD), which describes the intent/goal to "improve collaboration and interoperability" via:

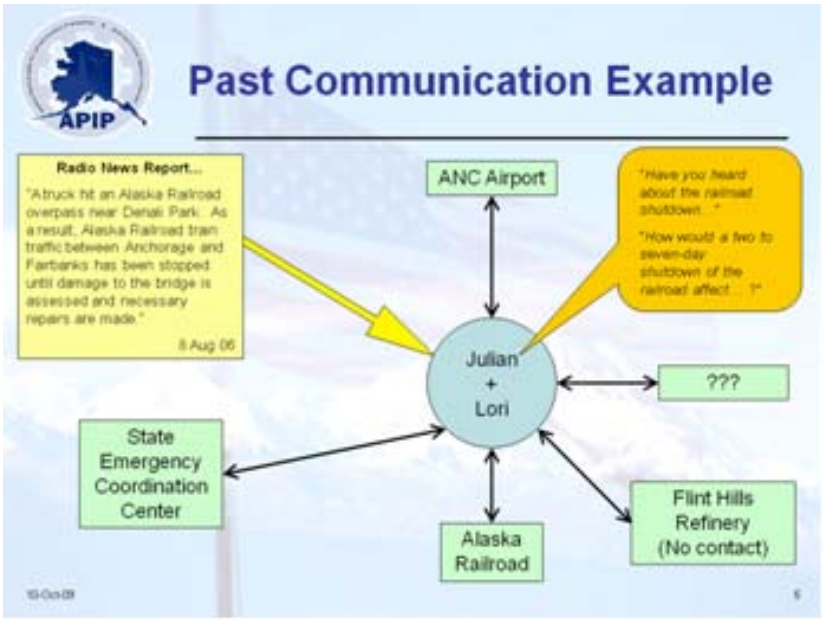

Figure 20. Past APIP Communication Example (From Martin, 2007, p. 5)

- Information sharing / information management
- Planning and response process improvement
- Resource management / resource typing
- Infrastructure sector characterization to understand vulnerabilities, dependencies, and single points of failure
- Cyber security
- Continuity of operations planning
- Team building and partnering. (APIP Charter, 2009, p. 1)

The above tasks would be accomplished by way of:

- Conducting infrastructure analysis to determine sector vulnerabilities
- Establishing infrastructure maps
- Sharing infrastructure information with APIP partners and other parties as required
- Providing a planning and response environment for critical infrastructure resource holders
- Developing internal communications procedures

- Making recommendations for priorities of protection, support and recovery
- Conducting various internal exercises and training opportunities (APIP Charter, 2009, p. 1)

The group also involved academic cohorts to help develop a process model that would survive day-to-day infrastructure changes related to personnel, backup functions, asset maintenance, etc. Once a process was in place, the group began to conduct infrastructure threat analyses based on identification of assets, vulnerabilities and dependencies. They looked across the sectors to define critical vulnerability interdependencies. The partners conducted tabletop exercises using realistic threat scenarios to define additional homeland defense and homeland security gaps and seams. The result of these efforts was a comprehensive list of integrated protection priorities for responsible law enforcement authorities. (Such forward thinking and practical application of knowledge would be useful in supporting Arctic region partners as well.)

It took years to develop the trust necessary for the partnership to allow government organizations to seek a collaborative solution that would respect proprietary data as well as solve information management and interoperable network issues impeding APIP's collaborative mission requirements. Using the policies provided at the national level for guidance, APIP began to look at technological solutions to enhance collaboration. The leaders wanted to reduce the investment risk by adopting a framework that was already developed and supported by organizations at the state and federal level, providing value added for "cheap." They were looking for real-time collaboration, reporting and chat, with a corresponding level of information security that was suitable to all partnership organizations. Since DHS was slated to be the primary point of contact for homeland security information sharing based on the *National Strategy for Homeland Security,* APIP leadership analyzed the DHS sponsored Homeland Security Information Network (HSIN).

Leaders discovered that HSIN was a ready-made collaborative tool that met their requirements and could also facilitate the gathering, analysis and distribution of relevant and actionable information needed to support their mission. The partners understood that they would still be required to invest their time by providing information, attending meetings and collaborating; technology would simply be a new means of sharing partnership data and knowledge. They also had to face a common challenge to effective data sharing: providing timely access to the right data in a usable format. Similarly, they recognized that collaboration also had to support performance management via standardized data collection and storage, shared databases and other technical resources (Imperial, 2004, p. 15).

In 2007, APIP leaders proposed using the state of Alaska HSIN portal page with an initial communication goal: “develop a system of alerting and reporting that enhances coordination between member organizations, sector leadership, and government agencies and results in improved mission assurance of critical infrastructure within Alaska” (Imperial, 2004, p. 15). APIP went on to develop a separate page inside the portal that is for use by members only to ensure that proprietary data is protected. New members can request access via the co-chairs of the partnership. Figure 21 shows the variety of pre-built, standardized advisory and situation report formats (company/sector assessments/incident status summary, etc.) initially provided to all APIP members within HSIN.

Figure 21. APIP HSIN Report Templates (From Martin, 2007, pp. 6-10)

Over the years, these five reports were condensed to two based on feedback from the partners as shown in Figure 22.

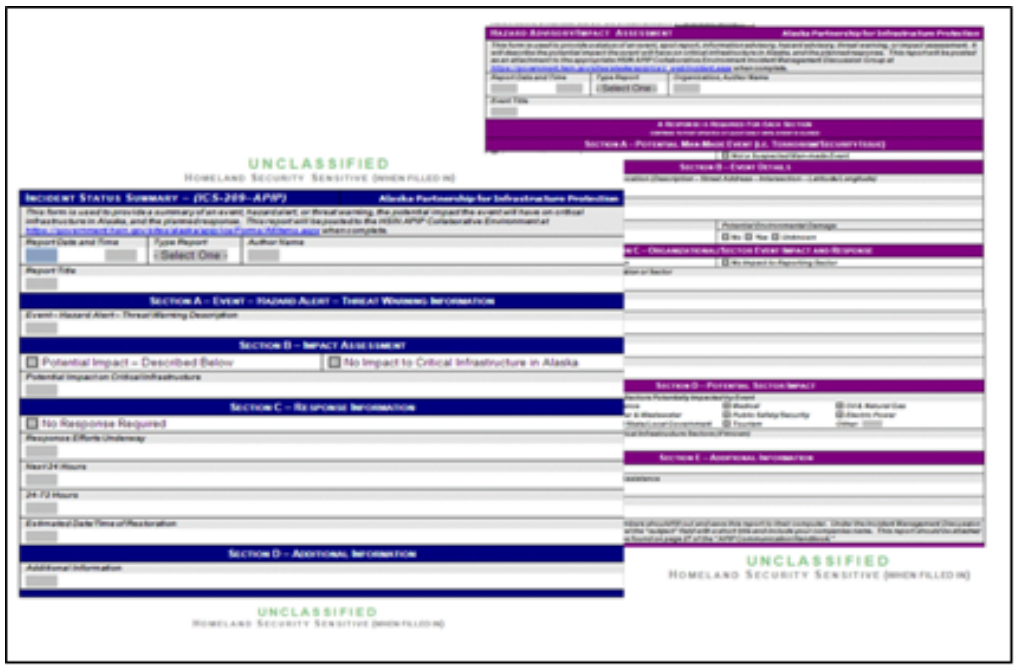

Figure 22. Incident Status Summary/Hazard Advisory Impact Assessment (From APIP, 2009, p. 12)

These APIP products cover initial reporting of incidents made by members that detail the event, its impact and response information (equivalent to the standard Incident Command System 209 form prescribed by FEMA.) The Hazard Advisory provides information on man-made events, threat warnings and impact to the sector and other members. The target audience for these products includes both the members and DHS who can monitor via the APIP portal on HSIN. APIP leaders also revised the coordinated process flow for information and set up automatic alert notices to APIP members (Martin, 2008). Members still had to figure out how to solve problems collectively, using shared data and subject matter expertise; however, the building blocks to facilitate such action were also made available.

In 2008, leaders provided refresher training with the goal that all participants understand how members "communicate with each other, select and fill out appropriate report template(s), effectively utilize HSIN and know how to get more information or assistance" (Jensen, 2008). In addition to developing processes for information sharing, they also developed handbooks for using the tool and continue to provide updates each year. Leaders provided partners with explicit guidance for data, reports and information flow to ensure collaboration and reduce frustration as shown in Figure 23 (APIP, 2009, p. 6).

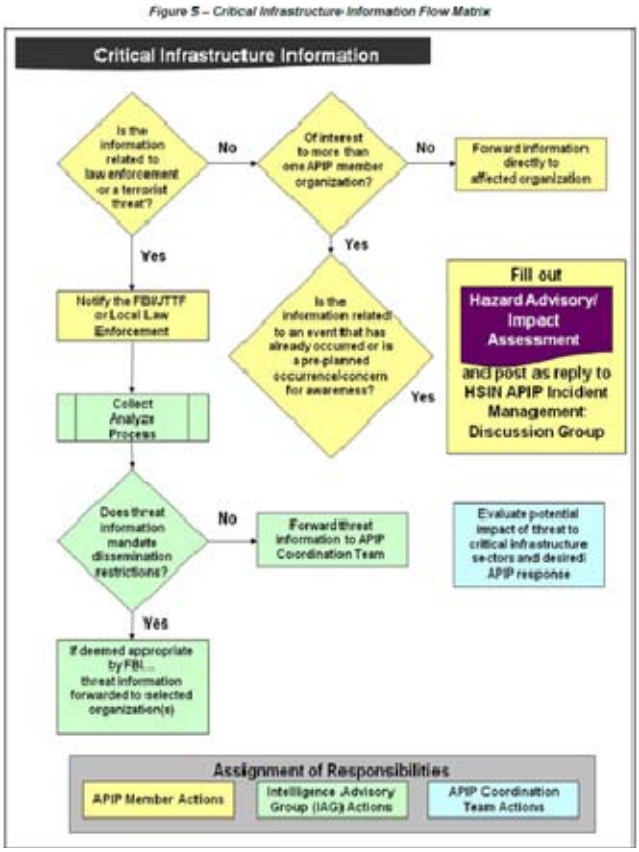

Figure 23. APIP Information Flow Responsibilities (From APIP, 2009, p. 6)

APIP has used HSIN over the years with great success, despite several reports citing difficulties with the system. For example, in 2006, the OIG cited five major issues for DHS regarding HSIN: 1) a clearly defined relationship between HSIN and existing collaboration systems, 2) lack of user requirements, 3) no evaluation of releases prior to implementation, 4) lack of user guidance to include clear information-sharing processes, training, and reference materials, and 5) missing baseline and specific performance measures leading to inability to track or assess information sharing (DHS Office of the Inspector General [DHS OIG], 2006, p. 3). The following year, GAO issued a report, stating DHS did not work effectively to:

> …fully develop joint strategies and policies, procedures, and other means to operate across agency boundaries, which are key practices for effective coordination and collaboration and a means to enhance information sharing and avoid duplication of effort. (GAO, 2007, cover)

In 2008, the DHS OIG issued a follow-up report on HSIN, making another five recommendations that included more resources, better stakeholder involvement/communication, developing scenario-based training, system performance/information-sharing metrics and defining/communicating information-sharing processes (DHS OIG, 2008, p. 1). Additionally, in 2008, GAO reported that DHS is acquiring a replacement system called *Next Generation HSIN* but has "not implemented key process controls in the areas of project and acquisition planning" (GAO, 2008, p. 2). GAO stated these processes include: developing a program office, requirements development and management, gathering, analyzing, and validating user requirements and risk management (GAO, 2008, p. 2).

A review of issues and recommendations in each of these reports indicate mainly program and resource issues at the federal level that have not necessarily prohibited effective use of the system by proactive practitioners. In fact, from an APIP perspective, the tool has worked "as advertised." Members have continued to use the system with the expectation that the federal government will continue to apply resources to protect users and their investment in the network. Likewise, members of the partnership see value in new features such as the *HSIN-Connect,* which will allow APIP to expand outside the local area using real-time Webinar-type collaboration for meetings and events.[10]

APIP members access their page inside the state portal each day (shown in Figure 24) and physically meet every third Thursday of the month during the APIP season, from September to May (APIP, 2009, p. ii). Partners have utilized the portal during real-world events that may impact infrastructure (power

[10] Information provided verbally from APIP chair.

outages, wildland fires, flooding, etc.) as well as during exercises using simulated threats. In fact, during a recent exercise, APIP members volunteered to participate in an exercise so they could provide additional reality to the scenario.

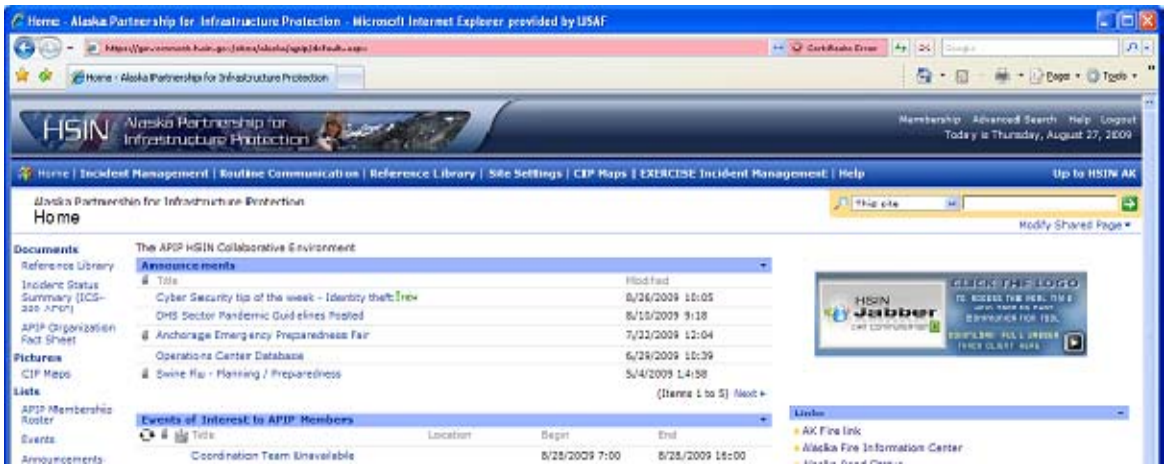

Figure 24. APIP Home Page (From APIP, 2009, p. 18)

This routine collaboration and robust mutual interest has helped overcome the lack of dedicated funding. (Similar to the AKIAC and JIACG, salary for partners comes from each respective organization. The distinction between these organizations and APIP is that APIP is a collateral duty for participants.)

According to members, the use of HSIN has supported the partnership for the past several years in four important ways.

- Cost. HSIN provides an effective means to collaborate at little to no cost. The portal's longevity is tied to Federal dollars, which are likely to last longer than local funding would, considering the current depth of state budget cuts.

- Customization. The use of HSIN as a generic, standardized tool allowed members to create and retain their own specializations, meaning that expertise is not blended into a process that focuses on one sector over another. Figure 25 highlights APIP's ability to tailor the site for incident management.

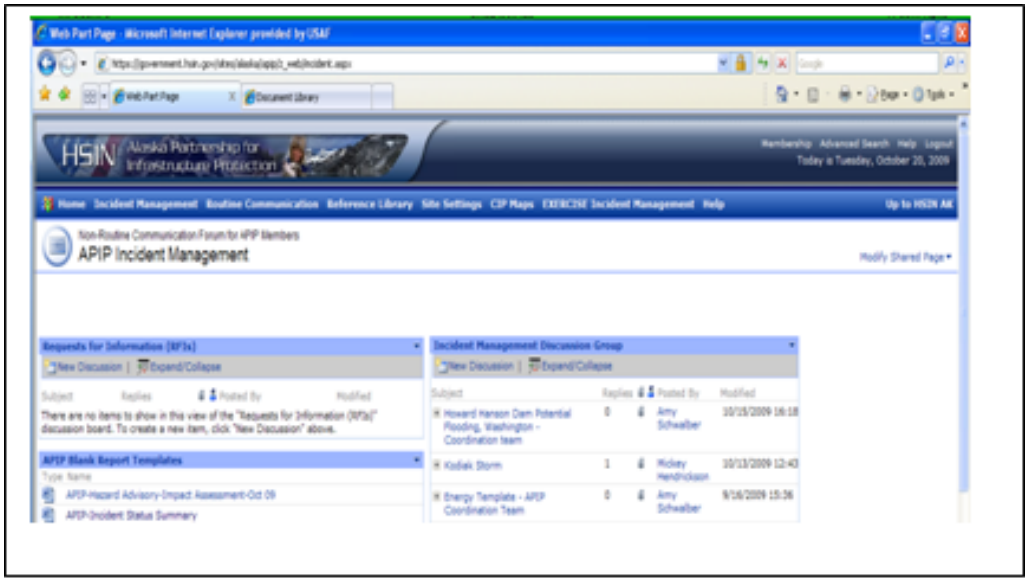

Figure 25. APIP Incident Management Page (From APIP, 2009, p. 19)

- Automation. HSIN delivers automatic alert notices to APIP members so they can immediately collaborate on a new event. This relieves staff members of the requirement to routinely monitor other organization's activities.

- Simplicity. APIP members recognized that complexity is already woven through their combined effort; they would have rejected a more complicated collaborative tool.

Over the years, the organizational makeup of APIP has grown to include communications, medical, oil refineries, emergency services, transportation, financial and water system sectors as shown in Figure 26. APIP members started attending Pacific Northwest Economic Region and Pacific Northwest Regional Emergency Management Assistance Compact exercises and meetings.

Figure 26. 2009 APIP Organization (From APIP, 2009, p. 2)

APIP was also acknowledged in two 2006 state HLS strategy (AKSHSS) objectives:

> 1) in partnership with Alaskan Command, continue to strengthen and extend the reach and influence of the Alaska Partnership for Infrastructure Protection (APIP) and,
>
> 2) Division of Homeland Security and Emergency Management continues to co-chair APIP and sector subcommittees, and the staff continues to assist APIP with development of communications plans, Emergency Operation Center (EOC) plans, exercise scenario development, exercise conduct and training. (State of Alaska, 2006, p. 4)

Five years after APIP's inception, the FEMA approved 2009 AKSHSS acknowledges the organization's continued expansion by stating that, "APIP provides a forum for the public and private sectors to share information and develop strategy for continuity of services including energy, medical services, and other vital sectors" (State of Alaska, 2009, p. 4). A corresponding objective is

to “develop a system for APIP members (InfraGuard) to share and provide recommendations on cyber infrastructure protection measures (State of Alaska, 2009, p. 14). Additionally, goal four of the AKSHSS is “strengthen information and intelligence sharing” with a corresponding objective to “continue to expand the use of the HSIN State portal” (State of Alaska, 2009, p. 15). Absent specific metrics, the growth, volunteerism, collaboration, products and daily use by members are indicators that the collective team believes their efforts are strengthening the resilience of the group as a whole. These are all value added propositions for Arctic policy partners.

In summary, the core success of APIP seems to be pinned on the persistence of those who believed in the requirement to share in the responsibility of protecting the infrastructure and the ability to leverage the HSIN portal. The focus on infrastructure protection and closed/limited portal leads to a low score in political acceptability; however, the processes, procedures, templates, frequency of collaboration, variety of partners and ability to make assessments gives APIP an overall high score as noted in Table 9.

Table 9. APIP Capability Analysis

APIP—Score 23/27 **Level of capability to meet the prescribed criterion**		
Low/Minimal	**Medium/Moderate**	**High**
1	**2**	**3**
Criterion 1.0 Robustness: Resources, Policies, Political Acceptability	**Criterion 2.0 Collaboration: Partners, Variety, Frequency**	**Criterion 3.0 Information Sharing: Systems, Processes, Procedures**
1.1 Available resources (Personnel, funding, i.e., ability to sustain effort)	2.1 Number of partners (few, some, many)	3.1 Systems used (Portals/Networks)
Score = 1 No dedicated funding/staff; participating organizations support with own staff (collateral duty for all)	Score = 3 Many partners/stakeholders	Score = 3 Use of HSIN collaborative system
1.2 Policies/Guidance	2.2 Level of collaboration	3.2 Processes for information

APIP—Score 23/27 Level of capability to meet the prescribed criterion		
Low/Minimal	**Medium/Moderate**	**High**
1	**2**	**3**
Criterion 1.0 Robustness: Resources, Policies, Political Acceptability	**Criterion 2.0 Collaboration: Partners, Variety, Frequency**	**Criterion 3.0 Information Sharing: Systems, Processes, Procedures**
(CONOPS, policy manuals, business rules, etc.)	(Federal/State/Local/Private Sector)	sharing/dissemination (templates, forms, contact lists, databases, etc.)
Score = 3 Charter/Handbook	Score = 3 Partnering at all levels	Score = 3 Many tested processes, templates
1.3 Political acceptability (Level of support or opposition)	2.3 Frequency of collaboration (daily, weekly, monthly)	3.3 Standard Operating Procedures (e.g. instructions for collecting and disseminating information)
Score = 1 Limited to / focused on infrastructure protection	Score = 3 Daily collaboration	Score = 3 Procedures in place for collecting data/making assessments

VII. CONCLUSION

The hypothesis in Chapter I was that an Arctic “community of interest” could leverage one of three popular information-sharing models: fusion center, Information Sharing and Analysis Center, or the Joint Interagency Coordination Group. Subsequent reviews were designed to determine which of the current working models was best suited based on the prescribed criterion. A recap of the outcome of these reviews and total scores assigned to each model is shown in Table 10.

Table 10. Capability Analysis Summary

Model and Final Score Summary (AKIAC=19 / JIACG=22 / APIP=23) **Level of capability to meet the prescribed criterion**					
Low/Minimal **Score = 1**		**Medium/Moderate** **Score = 2**		**High** **Score = 3**	
1		**2**		**3**	
Criterion 1.0 **Robustness: Resources, Policies, Political Acceptability**		**Criterion 2.0** **Collaboration: Partners, Variety, Frequency**		**Criterion 3.0** **Information Sharing: Systems, Processes, Procedures**	
Factors:		*Factors:*		*Factors:*	
1.1 Available resources (Personnel, funding, i.e., ability to sustain effort)		2.1 Number of partners (few, some, many)		3.1 Systems used (Portals/Networks)	
FC	1	FC	2	FC	3
JIACG	2	JIACG	3	JIACG	3
APIP	1	APIP	3	APIP	3
1.2 Policies/Guidance (CONOPS, policy manuals, business rules, etc.)		2.2 Variety of collaborators (Federal/State/Local/Private Sector)		3.2 Processes for information sharing/dissemination (templates, forms, contact lists, databases, etc.)	
FC	2	FC	2	FC	2
JIACG	2	JIACG	3	JIACG	2
APIP	3	APIP	3	APIP	3
1.3 Level of political acceptability (Level of support or opposition)		2.3 Frequency of collaboration (daily, weekly, monthly)		3.3 Standard Operating Procedures (e.g. instructions for collecting and disseminating information)	
FC	1	FC	3	FC	2
JIACG	1	JIACG	3	JIACG	3
APIP	1	APIP	3	APIP	3

The results show that there is less than a 10 percent difference between two of the models, and approximately 20 percent between the lowest and highest scores. These indicators suggest that a significant difference does not exist. In fact, all three models provide a certain amount of robustness, collaborative capability/partnerships and developed information-sharing processes. Likewise, all three models are weak in the area of "political acceptability," the level of support or opposition; meaning the degree to which "outside" organizations (other potential stakeholders) were included in the model's operational construct.

In each case the models were found to operate within their original domains or scopes of effort, which currently include law enforcement, natural disaster planning and infrastructure protection. This is likely due in part to the lack of specific mandates in the national and organizational level strategies. In other words, because these documents are not entirely prescriptive, a great deal of leeway exists for organizations to create partnerships and conduct information sharing as desired. Such freedom lets agencies tailor their needs to internally defined requirements and continue to "do business as usual." In hindsight, these results are a natural phenomenon that should not be too surprising.

While all three models advertise an inclusive approach to "all hazards" information sharing, it could be concluded that the AKIAC (fusion center) remains focused mainly on processing law enforcement/criminal data since only law enforcement personnel currently support that model. Likewise, APIP is focused on infrastructure protection and the JIACG on events impacting the private sector that could require a USNORTHCOM response. In general, none of the models are inclusive of all the hazards/domains necessary to capture the relevant data that would contribute to Arctic situational awareness. (While the national *Information Sharing Environment* envisioned pulling all domains/hazards into one collective setting, the full implementation of this effort remains to be seen.)

In essence, the hypothesis is false because none of the models provides a more complete "off the shelf" capability for use by Arctic partners/stakeholders than the others. More importantly however, the analysis reveals another dimension not fully considered in the criteria, which is the limited exposure each model has with respect to many of the DIMES entities. As described in the literature review, in addition to the military, information provided by the diplomatic (international partners/DoS), informational, (scientists/researchers/media) and economic (oil companies/shipping) entities would be necessary to develop full situational awareness in the Arctic. With the current limited focus of all three models, a significant amount of information relevant to Arctic homeland security/defense missions would be missing if any were to be adopted in their

current state of organizational existence. In other words, the ability to protect and secure the Arctic requires a complete image of the region; this would not be the case if any of the subject models were chosen.

It could be argued that these missing "stakeholders" (remaining DIMES entities) maintain a significant portion of the resident Arctic knowledge. The open source information that flows between these organizations would fill a tremendous gap in situational awareness of the Arctic community of interest. As one scholarly document claims, "It is important to not view information as a commodity; a better analogy would be that intelligence provides a nourishing meal, but open source information is the air that analysts breathe" (Henry L. Stimson Center, 2008, p. 42). In other words, those supporting defense/security will also need access to the information provided by the outlying contributors (all stakeholders) in order to be successful.

In summary, protecting the complex Arctic region requires an inclusive approach in order to provide full situational awareness. Such a community would support all the partners/stakeholders that provide, collect and produce information and products that contribute to Arctic security. The three models reviewed could be utilized as part of a larger community supporting Arctic policy. Three recommendations for building and sustaining such a community are provided below.

A. RECOMMENDATION 1. AN APPROPRIATE "CATALYST/CHAMPION" MUST PROMOTE A VALUE ADDED, INCLUSIVE INFORMATION SHARING "MEGACOMMUNITY"

By design, this researcher does not specify a person or organization as "the right one" to become the catalyst/champion(s) to develop an Arctic information sharing megacommunity of interest. Such a catalyst could in fact come from any number of stakeholders and/or equity partners. He/she (they) will intuitively recognize that an inclusive community offering more value than what is currently being produced by individual organizations is needed.

Figure 27 depicts a strategy canvas that could be used by the catalyst/champion to describe the enhanced value proposition as well as expected innovations that would lead to an increase in Arctic situational awareness.

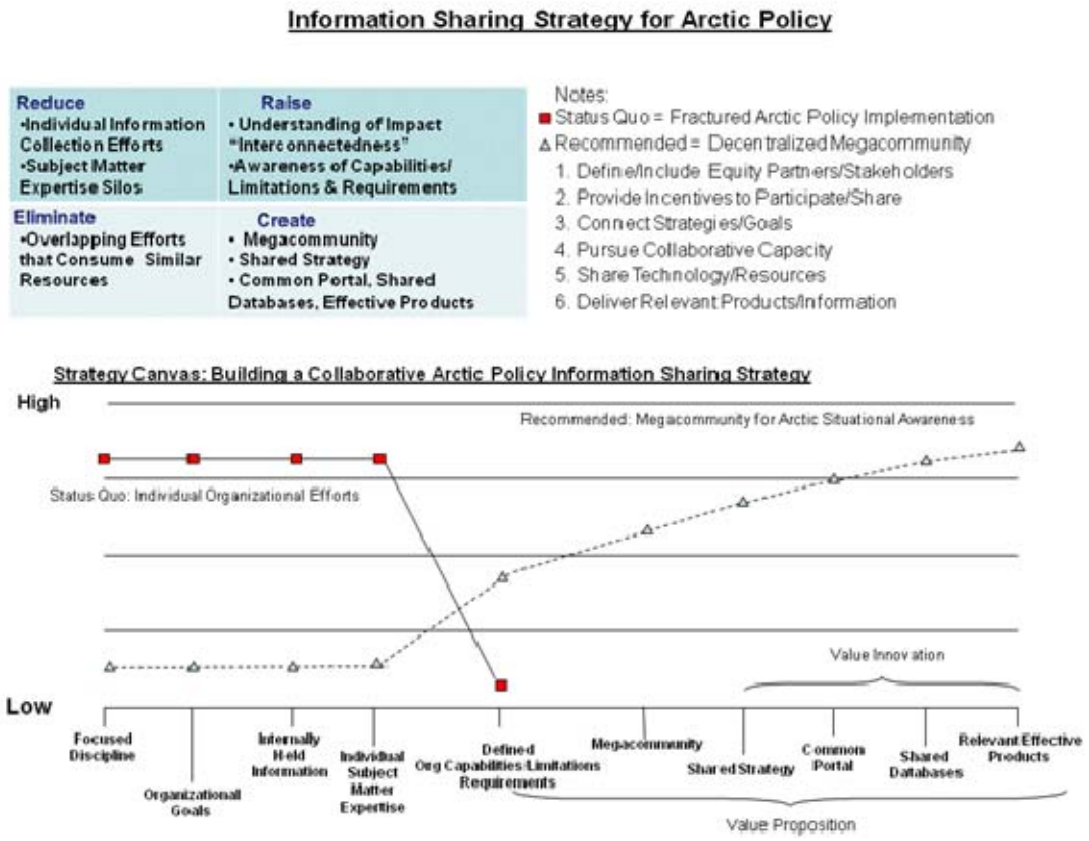

Figure 27. Strategy Canvas for Information Sharing in Support of Arctic Region Policy (After Kim & Mauborgne, 2005, p. 25)

Leveraging the canvas examples provided in *Blue Ocean Strategy*, the approach for Arctic Region Policy Information Sharing is described in the next three sections (Kim & Mauborgne, 2005).

1. Eliminate/Reduce

In the upper left corner of the strategy is a description of what needs to be eliminated and reduced based on the current situation (fractured Arctic Policy implementation—no existing, coherent strategy for sharing information). For

example, the strategy requires eliminating overlapping efforts that consume similar resources. In other words, the common and interdependent homeland security/defense issues would be discovered and documented for action, leading to a better understanding of the threats to the region. Likewise, a reduction in the amount of currently stovepiped (sharable) information and subject matter expertise would be released to provide value added for all members, leading to a more complete picture of the environment. Existing individual information collection efforts could be leveraged to build a shared knowledge base that supports all contributing organizations.

2. Raise/Create

The canvas continues with a description of raising awareness between all partners/stakeholders. This includes an understanding of capabilities, limitations, requirements and interests of each organization that could lead to an appreciation of "interconnectedness." As noted in one study, successful inter-organizational collaborative capacity includes, "...having a common goal or recognized interdependence...establishing and addressing goals for collaboration and considering the interest of other agencies in planning (Jansen, Hocevar, Rendon, Thomas, 2008, p. 13).

Discovering sympathetic relationships between organizations would naturally lead to the creation or "mashup" of an Arctic megacommunity that includes all the partners/stakeholders with an interest in securing the region. The authors of *Megacommunities* describe this concept as:

> …a public sphere in which organizations from three sectors—business, government, and civil society—deliberately joined together around compelling issues of mutual importance, following a set of practices and principles that make it easier for them to achieve results without sacrificing their individual goals. (Gerencser, Lee, Napolitano, Kelly, 2008, p. 53)

3. Grid

The bottom half of the graphic depicts how the two approaches map against the canvas. The status quo (current way of doing business) rates high with regard to interest in each specific discipline, individual organizational goals and individual subject matter expertise but drops dramatically, and in fact, stops before true collaboration begins. Likewise, the megacommunity approach is low initially because it minimizes individual aspects, adding value progressively as it moves towards incorporating shared portals, databases and products that contribute to situational awareness.

4. Megacommunity

While a natural tension is to be expected between the sectors based on organizational perspectives, building a megacommunity would bring organizations toward a shared sense of impact when/if something does go awry in the region. In other words, this complex, adaptive community would be in a continuous symbiotic learning cycle. These collective efforts will lead to shared resiliency—the ability of the community to absorb the impact of events, displacing individual, disconnected reactions. Likewise, based on a collaborative history, genuine commitment towards protecting the region would ultimately prevail over individual interests such as what the APIP organization experienced over several years of building habitual working relationships.

5. Value Innovation

A collective strategy would focus on collaborative contributions using a common portal and shared information databases that guide the development of effective, useful products. This may lead to challenges of sorting through volumes of constantly changing data, some immaterial or ambiguous. However, much of this could be negated by a development and understanding of proper procedures/utilization of information technology tools. Ultimately, a communal

knowledge base would be of value far beyond each individual contributor, ensuring a more secure environment that also satisfies Arctic region policy requirements.

The initial catalysts/champions would begin this process by defining the known equity partners and stakeholders from the tri-sectors. The first list would not be exhaustive and expected to grow as the community builds. A grid such as this would provide a framework within which the leaders could begin to map out the first members of the target community. This type of charting reminds leaders that protecting the Arctic will require information from many sources, in addition to the standard complement of governmental organizations such as DoD, DHS, and the state of Alaska. An example of initial importance and relevance of potential organizations is depicted in Figure 28.

Figure 28. Building the Arctic Region Megacommunity (From Gerencser, Lee, Napolitano, Kelly, 2008, p. 131)

In fact, the governmental organizations fall in the lower right quadrant of the graph as “more relevant” with regard to information needs due to their preventing and/or responding missions if an event occurs. By virtue of understanding the environment through science and daily operations, the

organizations depicted in the upper right are more important with regard to information sharing based on their subject matter expertise. This approach lines up with the elements of a knowledge base: understand the current knowledge (who has it), find out what we need to know and work on closing the gap between what we know and what we need to know (Gerencser et al., 2008, p. 147).

The grid includes the media since reporting on all aspects, whether economic, military, transportation or homeland security/defense will almost certainly be visible at a global level. As noted in the introduction, much of the national and homeland security political/military information on the Arctic is arriving via media reports. Shaping the informational environment with regard to Arctic policy partners/stakeholders internal and external interests may at times be in the hands of the media. Examples such as the sensational 2009 British tabloid *Mail Online* headline, *The Coldest War: Russia and U.S. Faceoff over Arctic Resource,* would not necessarily support the interests of the partners/stakeholders in the Arctic.

Likewise, including the mainstream public and environmentalist interests allows for information flow that is not necessarily resident with the "usual" partners and stakeholders. Such diversity would incorporate other perspectives and possibilities that would otherwise be ignored (Gorman, 2010). The authors of *Megacommunities,* highlight other reasons to include non-traditional members:

> …the civil sector brings accountability, insight into how to get things done locally, sensitivity to how the issues at play might affect individuals in the environment, and credibility in arenas in which business and government fall short. (Gerencser et al., 2008, p. 67)

As captured throughout this thesis, there are various organizations with vested interests in securing the Arctic. Each of these organizations is currently driven by political agendas and cultural/organizational motivation, inwardly focused on processes, and information collection/production. Similar to how the original stakeholders/partners will be mapped, the power and interest levels of each of these organizations will also need to be determined.

The power versus interest grid shown in Figure 29 provides a similar framework within which Arctic megacommunity leaders can determine where and at what level organizations may be expected to participate in the community. However, the true "power" resides in the community as a whole since none of the organizations will have all the answers or understand "how it is" given the complexity and constantly changing Arctic environment.

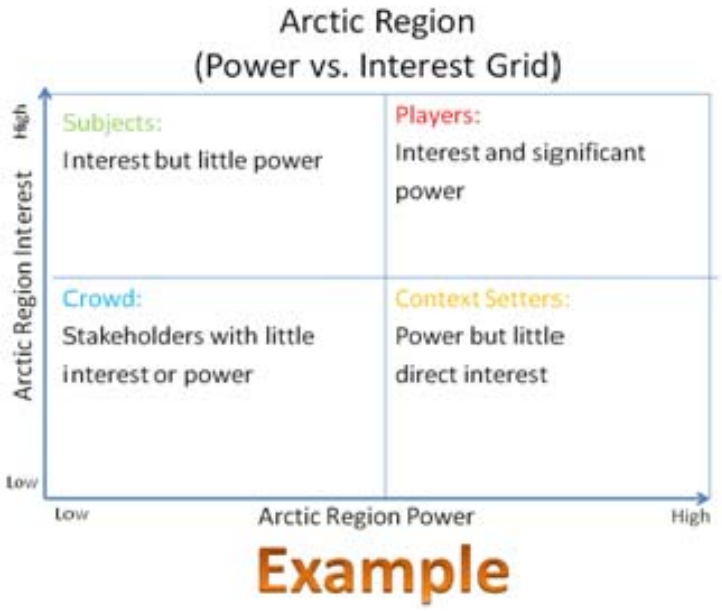

Figure 29. Arctic Region Power vs. Interest Grid (After Gerencser et al., 2008, pp. 124–138)

In addition to tri-sector engagement and overlapping vital interests, there also needs to be convergence, structure and adaptability (Gerencser et al., 2008). In this case, convergence means a commitment toward building security in the region. The community must take into account that the sectors may have different interests (proprietary/classified) that need to be respected. In other words, requirements will be dictated according to each organization's specific interests. Overall development of the community ("the plan") will come from the collective group to ensure an actionable strategy that includes implementable goals, milestones, protocols and principles that will benefit the entire community.

The community could operate under a simple structure initially, growing and adapting to new members and topics of interest, with follow-on planning for events, exercises, discussions and recurring (virtual) meetings that enhance the situational awareness of all members. Such up front activities would also allow organizations to become familiar with each other, helping to reduce the stress related to those partners who will be required to respond when/if an event occurs in the Arctic. As noted in the *Psychology of Terrorism*, "Extensive joint planning in conjunction with teamwork activity involving collaborating agencies can reduce the risk of experiencing adverse stress outcomes, particularly when responding in a multiagency context (Bongar, Brown, Beutler, Breckenridge, & Zimbardo, 2007, p. 239).

Finally, the group should consider how the communication network will be structured. The community could then take advantage of an information-sharing portal that would allow development of virtual connections using wikis, blogs, online forums and other social media tools. This would allow for the complete capture of the open source information-sharing capability that could be used during both routine and crisis operations. For example, the use of a tool such as the Ushahidi platform that "allows anyone to gather distributed data via SMS, e-mail or Web and visualize it on a map or timeline...to create the simplest way of aggregating information from the public for use in crisis response" (Ushahidi, 2010). Of course, leaders must take into account that some organizations may seek a totally open environment, while others may look for usernames and passwords to protect sensitive and/or proprietary information. Ultimately, the network needs will be based on member requirements and shaped to grow and adapt as the community expands.

B. RECOMMENDATION 2. USING AGREED UPON GOALS, TRUSTED LEADERS SHOULD FURTHER DEVELOP AND OPTIMIZE THE MEGACOMMUNITY'S INTERESTS

Once the Arctic megacommunity strategy is promoted by the catalyst/champion, the developed goals need to be supported and promoted by a

trusted leader. As noted by the author of *The Speed of Trust*, “world-class” trust consists of “...high collaboration and partnering, effortless communication, positive, transparent relationships with employees and all stakeholders, fully aligned systems and structures, strong education, engagement, confidence, and loyalty” (Covey, 2006, p. 24).

Such assurance must be inspired by leaders trusted at both personal and professional levels; those who arouse organizational trust for the entire community. A credible leader exuding integrity and appropriate intent will motivate Arctic megacommunity members to create value for each other; this in turn will cause production of something worthwhile that benefits the global citizenship. The leaders will also inspire subject matter expert working groups, increasing community value as problems are solved collectively. Those with opposing views will be encouraged to make their claims freely, knowing that leaders will consider their opinions and facts equally as part of the decision-making process.

Leaders will lightly shepherd this decentralized organization, encouraging members to contribute regularly and accurately. Such a construct allows for power distribution among all members, further encouraging development of a team/collective knowledge base. As noted by the authors of *Starfish and the Spider*, such an independent and autonomous organization (Arctic megacommunity) will resemble a circle without the hierarchy of centralized organizations (Brafman & Beckstrom, 2006, p. 88). Being part of this circle means that, “once you join, you're an equal. It's then up to you to contribute to the best of your ability” (Brafman & Beckstrom, 2006, p. 88). The interest and curiosity of the members will naturally drive community development. Good leaders will know when/where/how to “guide” the community as necessary and step back as members usher the organization towards its goals.

Guided by respected leaders, this open community will not rate one member at a higher level than another. In doing so, the inherent freedom will allow those participating to follow decided upon group norms in favor of more

rigid rules that accompany a typical centralized organization. Likewise, “when you give people freedom, you get chaos, but you also get incredible creativity” (Brafman & Beckstrom, 2006, p. 81). Such creativity/diversity will also support an innovative Arctic region defense that will look to not only keep pace, but gain on adversaries as they adapt to the changing environment. Trusted, flexible, “hands off” leaders will encourage community growth and added situational awareness for all members. Ultimately, those needing to protect the Arctic will be able to leverage these cultivated relationships and a library of information built by all megacommunity members. As noted in *The Age of the Unthinkable*, “This kind of self-organization, the ability to pull off an ‘all hands on deck’ reaction, exists in many of the most efficient and resilient systems in our world” (Ramo, 2009, p. 237).

In addition to trust, it will be a mutual ideology and stewardship that keeps the Arctic megacommunity focused on sustaining the organization. Collective interests and knowledge will also help relieve any contentious issues that arise. As long as the organization provides value added, members will continue to produce and seek to grow the community by pursuing additional relevant partners. If necessary, these online relationships can also be calculated. As described in *Measuring Public Relationships,* the successful use of social media can be quantified to a degree by reviewing data such as how many visits are made and how long the pages are viewed (Paine, 2007, p. 125). Likewise, counting the volume of conversations and number of comments could provide insight into how well a specific blog is received (Paine, 2007, p. 127). Several professional services are available to help review the quantity and quality of the online activity if the megacommunity believes that such statistics are value added.

C. RECOMMENDATION 3. LEVERAGE THE EXISTING RELATIONSHIPS AND CAPABILITIES OF THE INFORMATION SHARING MODELS REVIEWED

Leveraging the existing law enforcement partnerships of the Alaska Information Analysis Center, private sector subject matter experts in the Alaska Partnership for Infrastructure Protection and reachback to mission partners and other DoD organizations, provided by USNORTHCOM's Joint Interagency Coordination Group, could provide an initial boost in supporting the Arctic megacommunity.

For example, the AKIAC could pull information from the common portal, analyze and combine it with releasable intelligence that could be provided back to the community as products. Similarly, APIP has experience in developing portals, products, processes and procedures as well as relationships with many organizations that have an interest in the Arctic. Indeed, as existing partners, BP and ConocoPhillips would likely be major players in the megacommunity. As noted previously, the ties of these two organizations to the local communities go well beyond their status as simply "oil companies."

Likewise, as co-chair of APIP, the state of Alaska has developed connections to the native/tribal communities, who would also be major stakeholders in the megacommunity. Finally, the JIACG could provide information (policies, studies, exercises, etc.) and support from co-located organizations (established mission partners and other DoD organizations such as North American Aerospace Defense, missile defense agencies, etc.) to the Arctic megacommunity.

It should be noted that leveraging the "best practices" of these three organizations will require a better understanding of what each of those practices may be. The intent would be to use the momentum gained by each to jump start the megacommunity instead of reinventing some of the wheels. As noted by the author of *Smart Practices Research*, "treat the risks and uncertainties involved in adopting some seemingly smart practice as being on a par with the uncertainties

associated with all the other alternatives under consideration (Bardach, 2009, p. 109). In this case, with no other alternatives under consideration, leveraging these existing models would allow catalysts/leaders to begin by taking into account some relevant practices.

Finally, a recent scholarly article by a Nobel peace prize author on multi-scale approaches to climate change/collective action problems sums up the benefits of creating a self-organized community:

> A large number of variables increase the likelihood that self-organization could be effective in solving collective action problems. Among the most important are the following: (1) reliable information is available about the immediate and long-term costs and benefits of actions; (2) the individuals involved see the common resource as important for their own achievements and have a long-term time horizon; (3) gaining a reputation for being a trustworthy reciprocator is important to those involved; (4) individuals can communicate with at least some of the others involved; (5) informal monitoring and sanctioning is feasible and considered appropriate; and (6) social capital and leadership exist, related to previous successes in solving joint problems... The crucial factor is that a combination of structural features leads many of those affected to trust one another and to be willing to do an agreed-upon action that adds to their own short-term costs because they do see a long-term benefit for themselves and others and they believe that most others are complying. (Ostrom, 2010)

D. CONCLUSION

The 2009 *Arctic Region Policy* highlights the need to develop capabilities to protect U.S. air, land and sea borders, military/civilian vessels and aircraft, maritime commerce, critical infrastructure and key resources. The size and complexity of operating in this region was revealed in earlier chapters using a lens of economic, political/military and scientific activities and interest. Current information-sharing models are neither broad nor inclusive enough to support the level of effort necessary to provide full situational awareness. The ability to protect the Arctic will require information contribution from all partners and stakeholders, not just those traditionally thought of as security providers.

In essence, Arctic security is a “collective action/joint problem.” In the case of the megacommunity, once built, each organization will become familiar with ongoing issues in the region by way of access to reliable information. The megacommunity portal will become a trusted, common resource. Through this continuum of trust and shared knowledge, partners/stakeholders will invest in sustaining the effort. Participants will view the community as “their” resource, not something owned by any one organization, which will be another reason to contribute. The communication openness via freedom of input will enhance the value and when necessary, could be “informally monitored” by trusted leaders.

As previously stated, the intent of this chapter was twofold:

1. To inform the reader why the three existing information-sharing models fall short of supporting the partners/stakeholders in the complex Arctic region and,

2. To lay out recommendations for a way ahead, including a draft strategy.

Per the three recommendations made earlier, initial catalysts and subsequent leaders must create an Arctic megacommunity, leveraging existing models, partnerships, subject matter experts and all other organizations interested in Arctic region security. This community, particularly those with existing Arctic subject matter expertise, will be responsible for developing a plan of action/goals based on either the draft provided here or possibly their own strategic vision. This is a necessary and expected outcome of the inclusive megacommunity that forms. Only after considering all input and developing those goals (nourished by trusted leaders) will the collective group provide, collect and produce the information necessary for those expected to protect and defend the region.

Figure 30 provides a summary of what this community might look like. In the upper left is a diagram highlighting the overarching theme of “provide/collect/produce,” which intersects the functions supported by each

participating organization. In other words, organizations are expected to contribute so that information flows between each action circle.

(*Provide*/input into the community, *Collect* other data/information from the community, *Produce* some type of useful product back to the community.)

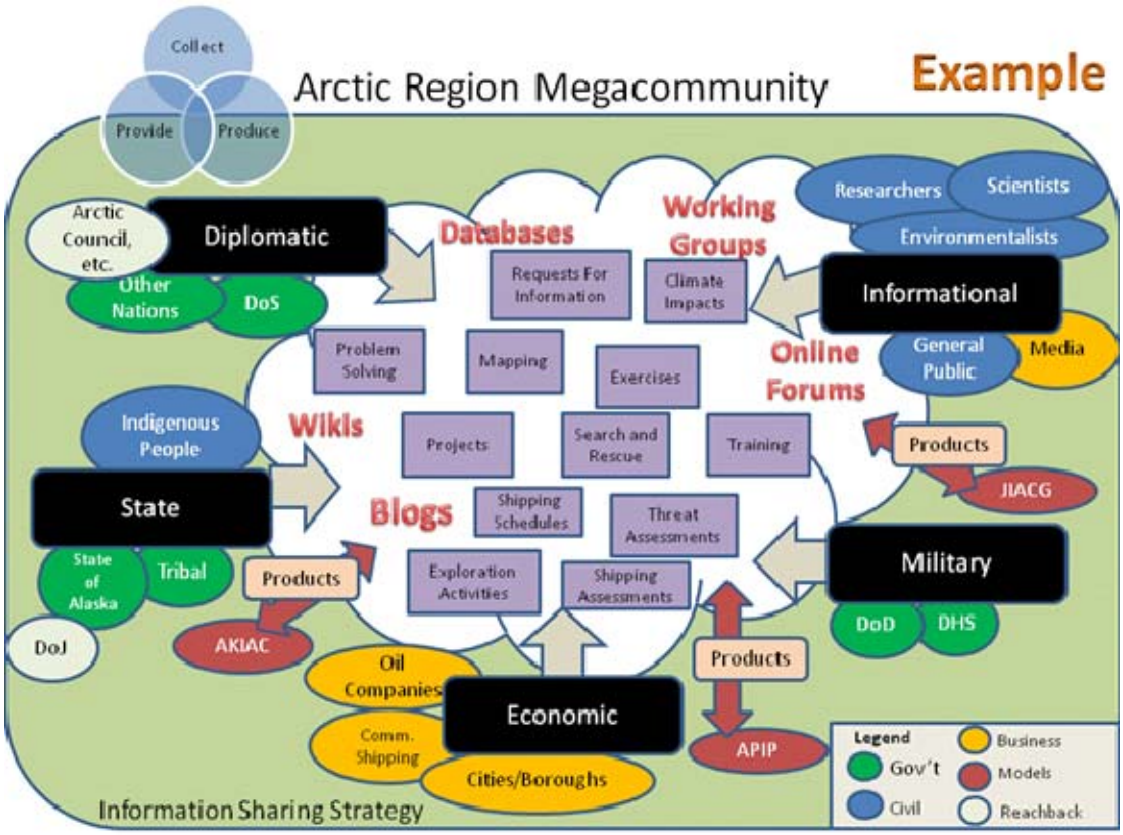

Figure 30. Information Sharing Strategy Summary

Surrounding the white "cloud of collaboration/portal" are the partners and stakeholders, clustered around the DIMES theme. The gray arrows show input collected from the partners/stakeholders going into the cloud. Inside the cloud are the collective actions that organizations may contribute to, depending upon their interests. For example, one organization may provide the shipping schedules for all traffic in the Arctic or the most recent climate survey. Another may contribute a database of all the types of ships that could traverse the Arctic or provide maps, so that in the event of a rescue, the community members would know what support they might need to provide to a response effort. Likewise,

scientists and the U.S. Coast Guard could blog their continental shelf mapping adventures or the community could construct a wiki that builds situational awareness for any number of Arctic areas of interest. As the community grows, natural themes will develop out of collaboration that will be recognized and supported by other participants.

The graphic also shows how the three models reviewed can extract data/information from the cloud to create products, which can then be reintroduced to the community in some fashion, depending upon the type of information contained. For example, the AKIAC could take a spot report provided by a community or ship, and combine that information with a related suspicious activity report and provide that product back to the community in an appropriate format. APIP could function similarly with an infrastructure report that might affect a response capability in the event of a ship in distress. Similarly, that partnership could provide specific infrastructure information to a community shouldering the Arctic that may need temporary support capabilities. These are examples of constructive ways that, as part of the community, the models, and other outside groups can cross-collaborate to minimize duplication of effort.

It has been made apparent that much of the data/information necessary to support situational awareness currently exists in many stovepipes. It will be up to the partners/stakeholders to migrate those “silos of expertise” into a megacommunity that will support the collective “intelligence” needed to protect the Arctic region. The resulting situational awareness picture will enable all responsible agencies to better defend the Arctic region and thus comply with the 2009 policy. The latest National Security Strategy hints at the importance of such a diverse, inclusive megacommunity to tie together all U.S. Arctic interests:

> The United States is an Arctic Nation with broad and fundamental interests in the Arctic region, where we seek to meet our national security needs, protect the environment, responsibly manage resources, account for indigenous communities, support scientific research, and strengthen international cooperation on a wide range of issues. (White House, 2010, p. 50)

Likewise, the President of the United States describes how we must strengthen our national capacity via a “whole of government approach” (White House, 2010, p. 14). This way ahead is focused particularly on building a “resilient” nation through both public and private sectors, and includes the strength of the general population as well. This approach is described further as:

> The ideas, values, energy, creativity, and resilience of our citizens are America’s greatest resource. We will support the development of prepared, vigilant, and engaged communities and underscore that our citizens are the heart of a resilient country. And we must tap the ingenuity outside government through strategic partnerships with the private sector, nongovernmental organizations, foundations, and community-based organizations. Such partnerships are critical to U.S. success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing. (White House, 2010, p. 16)

In conclusion, this thesis examined three currently existing information-sharing models to determine which would work best to achieve situational awareness for a broad array of Arctic partners and stakeholders. The thesis' research and analysis shows that no model is sufficient or stand-alone; rather a megacommunity is necessary, consisting of all equity partners (DoD, DoS, DHS, state of Alaska, etc.), interfacing with the stakeholders (researchers, private sector, media, etc.) and managed by leaders that will motivate the community to achieve a high degree of awareness for Arctic activity. Ultimately, protecting the complex Arctic environment and securing the top of the world will require a bottom’s up approach with participation from all partners and stakeholders. The next step is a call to action for a champion to take the lead, using this research as a springboard for future study.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Admiral T. J. Keating, USN Commander North American Aerospace Defense Command and United States Northern Command. Statement before the Senate Armed Services Committee. (2005, March 15). Retrieved April 2, 2010, from http://armed-services.senate.gov/statemnt/2005/March/Keating%2003-15-05.pdf

Alaska Information Analysis Center. *Alaska Information Analysis Center policy manual, 1*. (2009a). Internal document provided to author by center director, Anchorage, AK.

Alaska Information Analysis Center. (2009b). Concept of operations (Draft-4). 1. Internal document provided to author by center director, Anchorage, AK.

Alaska Legal Resource Center. (n.d.). *Alaska Statute AS 26.20.025: Creation and duties of the Alaska Division of Homeland Security and Emergency Management*. Retrieved September 20, 2010, from http://touchngo.com/lglcntr/akstats/Statutes/Title26/Chapter20/Section025.htm

American Association for the Advancement of Science. (1999). *The future of science and technology in Alaska: Other research organizations involved in Arctic research*. Retrieved July 2, 2010, from http://www.aaas.org/spp/cstc/pne/pubs/regrep/alaska/arctic.htm

Arctic Council. (n.d.). About. Retrieved July 2, 2010, from http://arctic-council.org/section/the_arctic_council

Arctic Council. (2009). *Arctic Marine Shipping Assessment 2009 Report*. Norway, Tromso: Norwegian Chairmanship. Retrieved July 2, 2010, from http://web.arcticportal.org/en/pame/amsa-2009-report

Arctic Energy for Today and Tomorrow. (2006). Retrieved May 21, 2010, from http://www.conocophillipsalaska.com/ArcticEnergy.pdf

Arctic Research Consortium of the United States. (n.d.a). *About ARCUS overview* Retrieved July 2, 2010, from http://www.arcus.org/arcus/index.html

Arctic Research Consortium of the United States. (n.d.b). *Directory of Arctic researchers*. Retrieved July 2, 2010, from http://www.arcus.org/

Bardach, E. (2009). *A practical guide for policy analysis: The eightfold path to more effective problem solving 2009.* Washington, DC: CQ Press.

Bloomfield, A. (2008, June 12). Russia plans Arctic military build-up in Moscow. *London Daily Telegraph*. Retrieved July 2, 2010, from http://www.telegraph.co.uk/news/worldnews/europe/russia/2111507/Russia-plans-Arctic-military-build-up.html

Bogdanos, M. (2007). *Transforming joint interagency coordination: The missing link between national strategy & operational success, case studies in national security transformation number 9*. Washington, DC: National Defense University, Center for Technology and National Security Policy.

Bongar, B. Brown, L. Beutler, L. Breckenridge, J. Zimbardo, P. (2007). *Psychology of terrorism*. New York: Oxford University Press.

Bowes, M. (2009, June 10). *Climate change: National security and the thawing Arctic*. Retrieved September 20, 2010, from http://www.star.nesdis.noaa.gov/star/documents/2009Ice/Day1/Filadelfo_Arctic-USNA_day1.pdf

Bowley, G. & Revkin, A.C. (2007, November 24). Icy Rescue as Seas Claim a Cruise Ship. New York Times. Retrieved July 2, 2010, from http://www.nytimes.com/2007/11/24/world/americas/24ship.html

Brafman, O and Beckstrom, R.A. (2006). The starfish and the spider: The unstoppable power of leaderless organizations. New York: Penguin Group

Brooks, G. (n.d). *Arctic Journal by RADM Gene Brooks*. Retrieved July 2, 2010, from http://www.uscgalaska.com/go/doc/780/230836/

Bryson, G. (2008, August 11). Receding ice pack means more traffic In Arctic. *Anchorage Daily News*. Retrieved July 2, 2010, from http://www.adn.com/news/environment/story/489973.html

Bryson, J. M. (2004). *Strategic Planning for Public and Nonprofit Organizations*. San Francisco, CA: Jossey-Bass.

Building on the information-sharing environment: Addressing challenges of implementation. (2006, May 10) Retrieved July 2, 2010, from http://www.fas.org/irp/congress/2006_hr/051006mcnamara.pdf

Canwest News Service. (2010, April 9). *Russia gets blasted over Arctic plans.* Retrieved July 26, 2010, from http://www2.canada.com/nanaimodailynews/news/story.html?id=968e2e5b-aee2-411b-99da-fa61735ee4b3

Catalino, J. (2009, March 6). *Private Sector Engagement.* Retrieved May 23. 2010, from http://www.same.org/files/public/TISP-SAME_Private_Sector_Brief030609.pdf

Catalino, J. & Hansen, D. (2009). *USNORTHCOM Private Sector Marketing Plan* (draft). Colorado Springs, CO: U.S. Northern Command.

Chertoff, M. Michael B. Mukasey. (2007, November 28). Letter to the Honorable Sarah Palin, Governor of Alaska, Juneau, AK. Provided to author by AKIAC Director.

Covey, S. M. (2006). *Speed of trust: The one thing that changes everything*. New York: Free Press.

Department of Defense. (2001). JP 1-02, *Department of Defense Dictionary of Military and Associated Terms, 290.* Washington, DC: author.

Department of Defense. (2005). *Strategy for homeland defense and civil support*. Washington, DC: author. Retrieved October 3, 2009, from http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf

Department of Homeland Security. (n.d.). State contacts & grant award information. Retrieved September 20, 2009, from http://www.dhs.gov/xgovt/grants

Department of Homeland Security. (2005a). National plan to achieve maritime domain awareness. Washington, DC: author. Retrieved October 5, 2009, from http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf

Department of Homeland Security. (2005b). *The national strategy for maritime security*. Washington, DC: author. Retrieved July 26, 2010, from http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf

Department of Homeland Security. (2010). *FY10 preparedness grant programs overview.* Retrieved May 7, 2010, from http://www.dhs.gov/xlibrary/assets/grant-program-overview-

Department of Homeland Security, Homeland Security Advisory Council. (2005). *Intelligence and information sharing initiative: Homeland security intelligence& information fusion*. Retrieved May 12, 2010, from http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf

Department of Homeland Security, Office of Inspector General. (2008). *DHS efforts to improve the homeland security information Network* (OIG 09-07). Washington, DC: author.

Department of Homeland Security, Office of Inspector General, Office of Information Technology. (2006). *Homeland security information network could support information sharing more effectively*. Washington, DC: author.

Department of Homeland Security & Department of Justice. (2008). Baseline capabilities for state and major urban area fusion centers. Washington, DC: authors.

Department of Homeland Security & Department of Justice. (2006). *Fusion center guidelines*. Washington, DC: authors.

Edwards, G. L. (2009). *Statement of Gary L. Edwards Chief Executive Officer National Native American Law Enforcement Association ("Nnalea") before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment "Homeland Security Intelligence: Its relevance and limitations."* Retrieved June 26, 2009, from http://www.fas.org/irp/congress/2009_hr/031809edwards.pdf

Ellis, B. (2009). *Arctic Marine Transport: Today & Tomorrow. 3rd Symposium on the Impacts of an Ice-Diminishing Arctic on Naval and Maritime Operations—US Naval Academy, 10 June 2009.*

Federal Emergency Management Agency & U.S. Department of Homeland Security. (2008). FY08 HSGP investment justification AK—State submission. Retrieved May 5, 2010, from http://www.ak-prepared.com/grant_forms/acrobat_docs/2008%20HSGP%20Statewide%20Investments.pdf

Federation of American Scientists. (1971). National Security Council, national security decision memorandum. Retrieved July 2, 2010, from http://www.fas.org/irp/offdocs/nsdm-nixon/nsdm-144.pdf

Federation of American Scientists. (1983). *National security decision directive 90, U.S. Arctic policy*. Retrieved July 2, 2010, from http://www.fas.org/irp/offdocs/nsdd/nsdd-090.htm

Federation of American Scientists. (1996). *Presidential decision directive/National Security Council—26 US Antarctica Policy*. Retrieved July 2, 2010, from http://www.fas.org/irp/offdocs/pdd26.htm

General V. E. Renuart, Jr., USAF, Commander United States Northern Command and North American Aerospace Defense Command, statement before the Senate Armed Services Committee. (2009, March 17). Retrieved September 20, 2009, from http://www.northcom.mil/news/Transcripts/090319.html

Gerencser, M. Lee, R., Napolitano,F., Kelly, C. (2008). Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together. New York: Palgrave MacMillan. Retrieved 28 March 2010 from http://www.northcom.mil/about/history_education/vision.html

Goman, C. K. (n.d.). *Strategies for inspiring workplace collaboration*. Retrieved July 3, 2010, from http://www.hodu.com/collaborate.shtml

Gove, D. (2009). U.S. Navy Arctic melt: Reopening a naval frontier. *Proceedings Magazine*, *135*(2), 272. Retrieved June 25, 2010, from http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1762

Government Accounting Office. (2006). *Critical infrastructure protection: Progress coordinating government and private sector efforts varies by sectors' characteristic.* (GAO-07-39). Washington, DC: author.

Government Accounting Office/ (2007a). *Federal efforts are helping to alleviate some challenges encountered by state and local information fusion centers*. Washington, DC: author. Retrieved May 5, 2010, from http://www.gao.gov/new.items/d0835.pdf

Government Accounting Office. (2007b). *Homeland security information network needs to be better coordinated with key state and local initiatives* (GAO-07-822T). Washington, DC: author.

Government Accounting Office. (2007c). *Report to Congressional committees, maritime transportation major oil spills occur infrequently, but risks to the federal oil spill fund remain* (GAO-07-1085). Washington, DC: author. Retrieved July 2, 2010, from http://www.gao.gov/cgi-bin/getrpt?GAO-07-1085

Government Accounting Office. (2008). *Management improvements needed on the Department of Homeland Security's next generation information sharing system* (GAO-09-40). Washington, DC: author.

Government Accounting Office. (2010). Report to Congressional requestors, *homeland defense DoD needs to take actions to enhance interagency coordination for its homeland defense and civil support Missions* (GAO-10-364. 27). Washington, DC: author.

Henry L. Stimson Center. (2008). *New information and intelligence needs in the 21st century threat environment* (Report No. 70). Retrieved June 19, 2010, from http://www.stimson.org/domprep/pdf/SEMA-DHS_FINAL.pdf

Honorable Sean Parnell Governor State of Alaska, Statement for the record "the strategic importance of the Arctic in U.S. policy" U.S. Senate Subcommittee on Homeland Security Appropriations. (2009, August 20). Retrieved September 20, 2010, from http://www.oceanlaw.org/downloads/Parnell_testimony-20Aug09.pdf

Imperial, M. T. (2004). *Collaboration and performance management in network settings: Lessons from three watershed governance efforts*. Washington, DC: IBM Center for the Business of Government.

Institute of the North. (n.d.). Retrieved May 21, 2010, from http://www.institutenorth.org/servlet/content/mission.html

Jansen, E., Hocevar, S., Rendon, R.G., & Thomas, G. (2008). *Interorganizational collaborative capacity: Development of a database to refine instrumentation and explore patterns* (SM-08-148). Graduate School of Business & Public Policy, Naval Postgraduate School, Monterey, CA.

Jensen, J. (2007, February 27). *Alaska partnership for infrastructure protection*. Presentation at SAME Conference, Anchorage, AK.

Jensen, J. (2008). *HSIN refresher training*. Presented to Alaska Partnership for Infrastructure Protection, Anchorage, AK.

Kim, W. C. & Mauborgne, R. (2005). *Blue ocean strategy: How to create uncontested market space and make the competition irrelevant*. Boston, MA: Harvard Business Press.

Klitgaard, R. & Treverton, G. (2003). *Assessing new partnerships: New forms of collaboration.* Santa Monica, CA: RAND Graduate School.

Kshemendra N. P. (2010). Program manager, information sharing environment annual report to the Congress. Retrieved April 25, 2010, from http://www.ise.gov/document/ISE_AR-2010_Final_2010-07-29.pdf

Letter from Governor Sean Parnell, State of Alaska to the Honorable Eric H. Holder, Jr. Attorney General and the Honorable Jane Napolitano, Secretary U.S. Department of Homeland Security. (2009, September 23). Document provided to author by Fusion Center Alaska Information Analysis Center, Anchorage, AK.

Marks, E. (2005). A work in progress [Letter to the editor]. *Joint Force Quarterly*, *39*(8).

Martin, D. (2007, April 2). *Communicating in the HSIN APIP Collaborative Environment*. Briefing to Alaskan Command/Joint Task Force Alaska, Anchorage, AK.

Martin, D. (2008, March). *HSIN refresher training*. Presentation to Alaska Partnership for Infrastructure Protection, Anchorage, AK.

McKay, J. (2008). *Statement of John McKay Former United States Attorney for the Western District of Washington before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment Committee on Homeland Security.*

McNamara, T. E. (2008). *Annual report to the Congress on the information-sharing environment*. Retrieved July 26, 2010, from http://www.ise.gov/docs/reports/Annual-Report-to-Congress-20080702.pdf

McNamara, T. E. (2009). *ISE progress and plans—Annual report to the Congress prepared by the program manager, information sharing environment*. Retrieved July 26, 2010, from http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_FINAL_2009-06-30.pdf

McNamara, T.E. (2008). *ISE enterprise architecture framework version 2.00*. Washington, DC: Program Manager, Information Sharing Environment.

National Fusion Center Coordination Group. (2009). *Primary and designated fusion centers*. Washington, DC: author.

National Oceanic and Atmospheric Administration. (n.d.). *Arctic theme page: research programs focused on the Arctic: Research institutions and organizations focused on the Arctic.* Retrieved July 2, 2010, from http://www.arctic.noaa.gov/research.html

NOAA star center for satellite applications and research, agenda 3rd symposium on the impacts of an ice-diminishing arctic on naval and maritime operations. (2009, June 9–12). Retrieved July 2, 2010, from http://www.star.nesdis.noaa.gov/star/IceSymposium2009Program.php

Northern Air Defense & U.S. Northern Command Interagency Coordination Directorate Joint Interagency Coordination Group (JIACG) strategy. [First draft, working document]. (2009, December 8).

Northern Air Defense & U.S. Northern Command Interagency Coordination Directorate. (2009). *Joint Interagency Coordination Group (JIACG) strategy* [First draft, working document].

Office of Naval Research, Naval Ice Center, Oceanographer of the Navy, and the Arctic Research Commission. (2001). *Naval operations in an ice-free Arctic symposium final report*. Retrieved September 20, 2010, from http://www.star.nesdis.noaa.gov/star/documents/2007IceSymp/FinalArcticReport_2001.pdf

O'Leary, R. & Bingham, L. B. (2007). *A manager's guide to resolving conflicts in collaborative networks*. Washington, DC: IBM Center for the Business of Government.

O'Rourke, R. (2010). *Coast Guard polar icebreaker modernization: Background, issues, and options for Congress* (RL34391). Washington, DC: Congressional Research Service.

Ostrom, E. (2010). A multi-scale approach to coping with climate change and other collective action problems. *Solutions 1*(2), 27–36. Retrieved June 25, 2010, from http://www.thesolutionsjournal.com/node/565

Paine, K. D. (2007). *Measuring public relationships: The data-driven communicators' guide to success*. Berlin, NH: KD Paine & Partners LLC.

PBS American Experience People and Events. (2006, April 4). *The Alaska pipeline U.S. and global oil consumption #11 of 13*. Retrieved July 2, 2010, from http://www.pbs.org/wgbh/amex/pipeline/peopleevents/e_consumption.html

Porter, R. M. (2009). *Statement of Russell M. Porter Director, State of Iowa Intelligence Fusion Center, Iowa Department of Public Safety; and General Chairman, the Association of Law Enforcement Intelligence Units (Leiu) before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment Committee on Homeland Security United States House of Representatives "the future of fusion centers: Potential promise and dangers."* Retrieved June 26, 2009, from http://www.fas.org/irp/congress/2009_hr/040109porter.pdf

Prepared Pursuant to Section 1016(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458). Retrieved July 2, 2010, from http://www.ise.gov/docs/reports/preliminaryreport.pdf

Ramo, J. C. (2009). *The age of the unthinkable: Why the new world disorder constantly surprises us and what we can do about it.* New York: Back Bay Books, Little, Brown and Company.

Rear Admiral Arthur Brooks, Commander, Seventeenth Coast Guard District, statement to the Alaska House State of Affairs Committee on the United Nations Convention on the Law of the Sea. (2009, March, 23). Retrieved July 2, 2010, from http://www.uscg.mil/cgjournal/message.asp?Id=121

Research Needs Work Group. (2009, June). *Recommendations on research needs necessary to implement an Alaska climate change strategy*. Retrieved September 20, 2009, from http://www.climatechange.alaska.gov/docs/rn_12jun09_dftrpt.pdf

Richter-Menge, J. & Overland, J. E. (Eds.). (2009). *Arctic report card update for 2009*. National Oceanic and Atmospheric Administration. Retrieved July 2, 2010, from http://www.arctic.noaa.gov/reportcard/ArcticReportCard_full_report.pdf

Russack, J. A. (2005). *Preliminary report on the creation of the information-sharing environment*. Retrieved July 26, 2010, from http://www.ise.gov/docs/speeches/testimonyrussack8nov.pdf

Secretariat on Sustaining Arctic Observing Networks. (n.d.). Sustaining Arctic Observing Networks [Brochure]. Retrieved May 16, 2010, from http://www.arcticobserving.org/images/stories/files/Final_Updated_SAON_Brochure.pdf

State of Alaska. (n.d.). *Alaska community database: Community information summaries.* Retrieved July 2, 2010, from http://www.commerce.state.ak.us/dca/commdb/CIS.cfm

State of Alaska Department of Administration, Division of Personnel, Emergency Management Study. (2004, December 16). *Memorandum, Deputy Director, Office of Homeland Security*. Retrieved September 20, 2009, from http://dop.state.ak.us/iscsi/OPD/Attachments/Studies/study_memos/DeputyDirectorOHSDec04.pdf

State of Alaska. (2009, November). *Governor Sean Parnell—100 Days* [Press release]. Retrieved April 25, 2010, from http://gov.alaska.gov/parnell/priorities.html

State of Alaska. (n.d.). *Division of Homeland Security and Emergency Management*. Retrieved September 20, 2009, from http://www.ak-prepared.com/homelandsecurity/

State of Alaska. (2009). *Homeland security strategy*. Retrieved September 20, 2009, from http://www.ak-prepared.com/grant_forms/acrobat_docs/Alaska_-_SHSS_-_2009.pdf

State of Alaska, Office of Management and Budget. (2009). *Homeland security grant program FY2010 request*. Retrieved September 20, 2009, from http://gov.state.ak.us/omb/10_omb/budget/DMVA/enacted/2010proj42901.pdf

Struck, D. (2007, August 7). Russia's deep-sea flag-planting at North Pole strikes a chill in Canada. *Washington Post Foreign Service*. Retrieved July 2, 2010, from http://www.washingtonpost.com/wp-dyn/content/article/2007/08/06/AR2007080601369.html

Struzik, E. (2010, May 23). Re-mapping Canada's Arctic. *Edmonton Journal*. Retrieved June 25, 2010, from http://www.edmontonjournal.com/technology/mapping+canada+arctic/3063320/story.html

Team Alaska. (n.d.). Alaska partnership for infrastructure protection charter. Anchorage, AK: State of Alaska & Alaskan Command/Joint Task Force Alaska. Retrieved July 26, 2010, from http://www.ak-prepared.com/apip/documents/APIP%20Charter.doc

Team Alaska. (2009, September 15). Alaska partnership for infrastructure protection communication handbook. Anchorage, AK: State of Alaska & Alaskan Command/Joint Task Force Alaska.–

Teeple, N. (2010). A brief history of intrusions into the Canadian Arctic. *Canadian Army Journal*, *12*(3), 52.

Treadwell, M. (2009, March 3–6). *U.S. Arctic Research Commission, UNESCO experts meeting: Sustainable development of the Arctic in the face of global climate change: scientific, cultural and educational challenges, Monaco*. Retrieved July 2, 2010, from http://www.unesco.org/csi/LINKS/monaco-ppts/Treadwell_ppt_MonacoUNESCOarctic.pdf

United Press International, (2010, May 3). *Russia Invites China to Explore Arctic.* Retrieved July 26, 2010, from http://www.upi.com/Science_News/Resource-Wars/2010/05/03/Russia-invites-China-to-explore-Arctic/UPI-40391272903186/

University of the Arctic Institute for Applied Circumpolar Policy, Dickey Center for International Understanding at Dartmouth College and the Carnegie Endowment for International Peace University of the Arctic. (2009, July 7). *UArctic co-sponsors international security report*. Retrieved July 26, 2010, from http://www.uarctic.org/singleNewsArticle.aspx?m=83&amid=7497

Ushahidi. (n.d.). Retrieved July 5, 2010, from http://ushahidi.com/

U.S. Air Force. (2009, June 26). *Agreement signed for integrated defense of Alaska*. Retrieved October 2, 2010, from http://www.af.mil/news/story.asp?id=123156142

U. S. Coast Guard. *Arctic overview brief*. Retrieved September 20, 2010, from http://www.uscg.mil/D17/ArcticOverview.pdf

U.S. Coast Guard. (2008). U.S. Coast Guard Arctic strategic plan (draft). Retrieved September 20, 2010, from http://www.uscg.mil/hq/cg5/cg513/docs/Draft_CG_Arctic_Strategic_Plan_12012008.rtf

U.S. Coast Guard. (2008). *Circum-Arctic resource appraisal: estimates of undiscovered oil and gas north of the Arctic Circle* [Fact sheet]. Retrieved May 21, 2010, from http://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf

U.S. Energy Information Administration. (2008). *Petroleum products consumption*. Retrieved May 21, 2010, from http://www.eia.doe.gov/neic/infosheets/petroleumproductsconsumption.html

U.S. Energy Information Administration. (2010, January). *Independent statistics and analysis. 2008 petroleum basic statistics*. Retrieved May 21, 2010, from http://www.eia.doe.gov/basics/quickoil.html

U.S. Joint Forces Command. (2007). *Commander's handbook for the Joint Interagency Coordination Group*. Washington, DC: U.S. Joint Forces Command, Joint Warfighting Center, Joint Innovation &Experimentation Directorate

U.S. Joint Forces Command. (2005, January). *JIACG fact sheet*. Retrieved March 28, 2010, from http://smallwarsjournal.com/documents/jiacgfactsheet.pdf

U.S. State Department. (n.d.). *Establishment of the Arctic Council*. Retrieved June 20, 2010, from http://www.state.gov/g/oes/ocns/opa/arc/ac/index.htm

White House. (2010, May). *National security strategy*. Retrieved June 25, 2010, from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

White House, Office of the Press Secretary. (2009). *Homeland security presidential directive 25*. Washington, DC: author.

White House, Office of the Press Secretary. (1998). *Homeland security presidential directive NSC-63*. Retrieved January 12, 2010, from http://ftp.fas.org/irp/offdocs/pdd/pdd-63.htm

White House, Office of the Press Secretary. (2009). *National Security Presidential Directive 66*. Washington, DC: author.

Xinhua News Agency. (2010, July 21). *China's icebreaker "snow dragon" sails across Arctic Circle.* Retrieved July 26, 2010, from http://news.xinhuanet.com/english2010/photo/2010-07/21/c_13407659.htm

Yalowitz, K.S., Collins, J. F., & Ross, A. V. (2008, December 1–3). *The Arctic Climate Change and Security Policy Conference final report and findings*. Dartmouth College, Hanover, NH.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California